PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERIA

MAESTRÍA EN REDES DE COMUNICACIONES

"ESTUDIO DE UN SISTEMA DE PREVENCION DE INTRUSIONES BASADO EN REDES NEURONALES; PROPUESTA DE DISEÑO UNIDAD EDUCATIVA BRETHREN"

TESIS DE GRADO PRESENTADA COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE MÁSTER EN REDES DE COMUNICACIONES

AUTOR: FABIÁN PAUCAR.

DIRECTOR: ING. DAVID RAMIREZ MSC.

QUITO ABRIL 2015.

Declaración

Yo, FABIÁN RAFAEL PAUCAR GUAMÁN, declaro bajo juramento que el trabajo aquí descrito de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración, cedo los derechos de propiedad intelectual correspondiente a este trabajo, a la Pontificia Universidad Católica del Ecuador, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normativa institucional vigente.

_____

Fabián Rafael Paucar Guamán

Certificación

Certifico que el presente trabajo fue desarrollado por Fabián Rafael Paucar Guamán bajo mi supervisión.

_____

Ing. David Ramirez MsC.

Director del Proyecto

Dedicatoria

Quiero dedicar la presente principalmente a Dios y entre tantas personas a las que más me apoyaron en el trayecto de la realización de mi objetivo.

Con todo cariño: a mi madre, mis hijos.

Agradecimientos

El siguiente trabajo está dedicado con la máxima expresión de gratitud.

A mis distinguidos maestros, que con nobleza y entusiasmo dedicaron el día a día, para verter sus apostolados en mi mente.

Y a mí estimada Pontificia Universidad Católica del Ecuador, porque en la acogida de sus aulas recibí las más gratas enseñanzas que nunca podré olvidar.

Contenido

Lista de tablas

Lista de figuras

CAPÍTULO I

1.1 Introducción

La tecnología avanza a cada momento a pasos agigantados, aquello ha provocado que el ser humano tenga que estar a la vanguardia en aspectos tecnológicos, específicamente en redes informáticas mismas que son importantes puntales en la comunicación de hoy en día, y gracias a esto la productividad de un país avanza en función a las necesidades que requiera satisfacer, de igual manera, como todo mejora en bienestar de uno o varios conjuntos de personas; también existe el caso de los individuos que buscan el perjuicio de la comunidad, y a su vez otros que resuelven construir beneficios para sí mismos dentro de la competencia, logrando ubicarse a la cabeza con estrategias que van en contra de la comunicación. En ocasiones construyen software básico para alterar el funcionamiento de una red o crean grandes estructuras, procurando darse a conocer como empresa de desarrollo o en búsqueda de información que sea de su interés, haciéndolo para dañar a la competencia o lucrar en forma ilícita. Debido a lo mencionado, existen personas que desarrollan tecnologías para dar seguimiento a estos técnicos, corregir y evitar con tiempo adecuado y prudencial la ruptura de los procesos informáticos creando en dicho caso filtros que den o no paso a determinada información, que se encuentra etiquetada por determinado software para establecer parámetros y seguridades dentro de un sistema, de esta forma buscan evitar desastres en una institución con respecto a la perdida de “información”.

En este contexto se presentará un estudio y análisis de ataques y cómo prevenirlos, al someter tráfico a filtros de inspección de información denominados Sistemas de Prevención

de Intrusos (SPI) basado en clasificar la información a través de Redes Neuronales Artificiales que de ahora en adelante la llamaremos (ANN), para esto se detallan sus tipos, características, técnicas, ventajas y desventajas al ser utilizadas y al combinarlas con los SPI, resaltando la implementación en una institución educativa con la intención de verificar los resultados que se encuentran al hacer pruebas por ejemplo las entradas, payload y cabeceras de protocolos TCP, UDP, IP, entre otros., adicionando a esto que el interés primordial es dar a conocer el uso de estas y como es su funcionamiento al ser la red conectada principalmente a internet, utilizando herramientas adicionales para el manejo de procesos de seguridad y análisis de tráfico.

1.2 Antecedentes

Al iniciar cualquier empresa lo primero que se planifica es la comunicación entre pares en red, que garanticen la transmisión de la información, sin embargo si no se toma en cuenta que existen individuos u organizaciones buscando la oportunidad de obtenerla de forma ilícita, tomando en cuenta que muchos de los procesos transmitidos suelen parecer normales a trabajo que se realiza a diario.

La inmadurez que se tiene en la Seguridad de Información (SI) y en los Sistemas de Red Emergentes (ENS) provoca que las vulnerabilidades de los sistemas sean fáciles de identificar y atacar en una red, a sabiendas que los dispositivos de concentración del tráfico representan cajas negras como lo menciona el Instituto de Ingeniería de Software (CERT) en su post indicando que estos en la mayoría son desdeñosos y puesto que la domótica en un

futuro busca implementar proyectos con inteligencia artificial, si no se los toma en cuenta serán puntos de apoyo para los atacantes.

"La comprensión de los protocolos de comunicación utilizados por un sistema es vital para identificar vulnerabilidades explotables remotamente".

Ante esto propone técnicas analizadas para el descubrimiento de vulnerabilidades. (Householder, 2014)

Además de las políticas de seguridad se toma en cuenta que gran parte de las personas en la actualidad realizan sus estudios a partir de la web a lo cual se ha creado plataformas como Moodle, E-learning entre otras que permiten la educación de los individuos desde lugares lejanos sin embargo es un foco de atención para los atacantes como lo menciona la Revista Seguridad – Defensa Digital en su nota Ciber seguridad para la Educación On-Line indicando que la demanda educativa es un llamado de atención para las configuraciones de seguridad y entidades de soporte, que proponer y ejecutar por las plataformas universitarias en línea sin filtros es un gran error (Valencia, 2014), y que para especificar seguridades dentro de una red cabe mencionar que es necesario implementar reglas que permitan controlar el tráfico dentro de la misma, esto se lo realiza a través de firewalls tomando en cuenta que se debe conocer su core y que este se menciona en diversas interfaces gráficas para su manejo como es el caso del articulo propuesto por Microteknologías indicando su función, utilidades, beneficios y posibles interfaces para efectuar en las redes, adicionando que existen un muchas webs que indican cómo manejarlas de las cuales algunas son proporcionadas por ejemplo vía doc.ubuntu-es. (Aliyev, 2015), dicho esto se menciona que

al implementar un firewall dentro de una red se vigila cierta cantidad de tráfico sin embargo existe código malicioso al cual no se puede solamente controlar con reglas, según la tesis de posgrado propuesta por Alberto Álvarez Oliva se puede configurar IDS, ejemplo Snort el cual permite al ser identificadas las vulnerabilidades de un sistema conocer las cabeceras de los paquetes de tráfico en la capa de red siendo este un sniffer que permite detectar ataques y barridos de puertos (Oliva, 2013). Según CISCO el acceso unificado es una innovación inspirada en la sencillez adicionando que este demuestra que cada vez más los usuarios manejan la movilidad con el aumento de dispositivos por empleado de una empresa a lo cual también agrega mayores desafíos para la seguridad y administración de las Tecnologías de Información(TI), y que la movilidad crece en altos grados, lo mismo ocurre con el acceso a la nube, debido a esto CISCO calcula que podríamos llegar casi a los 30 mil millones de dispositivos para el año 2020, de igual forma busca unificar las redes para poder administrarlas y mantenerlas seguras de forma sencilla con una sola política y en una sola red CISCO Unified Access en su artículo menciona también nueva arquitectura que pone en venta para mejorar la administración y seguridad de las TI siendo este un desafío para las empresas puesto que tendrían que cambiar los equipos tradicionales, si esto llega a implementarse en las empresas los niveles de seguridad darían un giro de 180^0 (Mehra, 2013).

Según la tesis propuesta por José Daniel Britos acerca de la detección de intrusiones en redes de datos se busca mejorar los métodos de detección de ataques proponiendo nuevas arquitecturas analizadas para implementación a través de algoritmos propuestos mediante el

uso de herramientas IDS. (José, 2010), adicionalmente se sabe que la suite de protocolos TCP/IP tiene vulnerabilidades en sus procesos a lo cual Marcelo Riffo propone identificar vulnerabilidades y diferentes mecanismos de prevención y protección, en su trabajo de tesis realizado para la Universidad de Valdivia de Chile (Riffo Gutierrez, 2009), de igual manera para obtener una protección adecuada de los procesos de una red al generar tráfico es conveniente analizar, modificar, probar y ejecutar sistemas existentes de seguridad informática, lo que presenta en su proyecto María Isabel Giménez García al implementarlo en la Universidad de Almería para clasificar su utilización y escoger la mejor herramienta, en un entorno de red real buscando el rendimiento adecuado y adaptación tomando en cuenta que realiza estudios de Sistemas de Detección y Prevención de Intrusos con sus características. (García, 2008), existen muchos documentos que describen métodos de implementación de seguridad para una red que pueden ser analizados como base para nuevos proyectos como es el caso de la tesis "Modelo de seguridad para la medición de vulnerabilidades y reducción de riesgos en redes de datos" de Erick Cruz y Diana Rodríguez en la cual también se indica solo como propuesta pasos para facilitar la administración de la red a través de software dedicado(Cruz Erik, 2010). Para realizar un análisis de vulnerabilidades en una red lo primordial es tener en cuenta que por dicha red se transmiten diversas cantidades de información, por lo tanto es indispensable realizar un análisis exhaustivo del tráfico que se transfiere como es el caso del Sistema de monitorización y análisis de tráfico para la Anella Científica de SMARTxAC el cual presenta detalles estadísticos del uso de la red y la descripción de sus componentes en tiempo real para redes

troncales (P. Barlet, 2004), el caso por ejemplo del artículo “Metodología para el análisis de tráfico de una red de transmisión de datos” el cual propone métodos de análisis de redes a través de la simulación de las mismas siendo uno de los ejemplos exitosos al monitorear tráfico (Mok, 2002), según artículos y material de búsqueda de vulnerabilidades propuesto por la compañía Tech Target se puede obtener altos niveles de seguridad tomando en cuenta la gestión para aplicarlos como son evaluaciones, pruebas, hacking ético y parches (Target, 2000 -2015), procurando dar a entender de una mejor manera acerca de cómo se provocan los ataques dentro de una red tanto a los sistemas, dispositivos y a unos cuantos protocolos y describir sus vulnerabilidades ya conocidas se describen en el libro Análisis de Seguridad TCP/IP de Raúl Siles, el cual permitirá de una mejor manera entender cómo operan determinadas técnicas en contra de una red (Siles R., 2002).

Ya teniendo en cuenta como realizar monitoreo y captura de paquetes a varios niveles de red es conveniente optar por una solución con tecnologías más robustas que permitan detectar y prevenir intrusiones como es el caso de identificación de ataques por medio de redes Neuronales.

Con el estudio de la inteligencia computacional a base de representaciones ontológicas se ha logrado encontrar nuevos caminos para mejorar las reglas para la detección de ataques realizados por instrusos como lo menciona en su articulo IZA Gustavo A y demás, presentando resultados de sistemas orientados a la detección de intrusos y con sus características e integrando arquitecturas diversas para mejorar la capacidad de identificación de patrones de ataque a diferencia de los IDS estandar. (Iza Gustavo A, 2009).

Al conocer nuevas tecnologías como es el caso de las Redes Neuronales Artificiales es muy importantes describir sus características, ventajas, desventajas, e implementaciones de la mayoría de estas y que mejor si se las demuestra realizando aplicaciones, se cita en este caso con el trabajo aplicado al análisis de datos basandose en la Psicología realizado por Juan José Montaño Moreno obteniendo como resultados sobre el 99% exitosos al investigar individuos consumidores de extasis, apegandose a errores que pueden parecerse a las redes clasicas (MORENO, 2002), a mas de esto es importante conocer en forma general la composición de una red neuronal artificial como se describe en el video presentado por Javier García sobre todo si es explicado desde un inicio. (García J. , 2012). Es importante conocer que un sistema de detección de intrusos puede adaptarse a una red neuronal a través de procesos analizados previamente para su implementación como es el caso de la tesis realizada por Juan León Henao Ríos en la cual encuentra resultados obtenidos de una matriz de 64 elementos de los paquetes analizados como datos de entrada y un 89% de confiabilidad para detectar intrusiones. (León, 2012), por último se presenta la tesis implementada en el Municipio de Riobamba buscando proteger su red a través de un Sistema de prevención de Intrusos obteniendo resultados satisfactorios sobre este. (Torres A. Gabriela C., 2010)

Según lo analizado en diferentes documentos se encuentra que existe diversa información acerca de la seguridad en las redes, IDS y aplicaciones a Redes Neuronales planes y metodologías para proteger a través de hardware o software el tráfico que fluye por la red, pero existe poca información acerca de IPS basado en Redes Neuronales los cuales convierten a este trabajo en un reto a desarrollar.

1.3 Justificación

En la mayor parte de casos, las instituciones cuentan con sistemas interconectados en red, los cuales a medida que suelen ser utilizados sufren ataques de diversa índole, dentro de la misma teniendo en cuenta que para muchas la información transmitida es muy esencial, es decir su patrimonio en sí.

Es importante que antes de poner en funcionamiento la información en una red se considere que ésta debe disponer de una infraestructura de protección a base de procesos y técnicas, buscando los mejores planes y opciones que le permitan brindar seguridad al tráfico proporcionado por cada estación o servidores en forma privada o al tener que salir al internet y de la misma manera al ingresar tráfico externo a dicha red.

La escasez de personal calificado para estar monitoreando información y los costos infructuosos, implican ubicar técnicos para vigilar la red, con lo que también se obliga a buscar dispositivos que permitan controlar de manera inmediata, directa y de bajo costo todo el tráfico transmitido procurando obtener filtros para permitir o no ciertos contenidos recurrentes dentro de la mencionada red, la información que se obtiene de internet debe ser controlada aún más, puesto que trae subrutinas inadecuadas para infraestructuras que no deben estar en una red privada, y estas es vital para muchas instituciones, además se debe tener conocimientos sobre el tipo de información que se está transmitiendo, de ser así será una gran ventaja para cualquier establecimiento, esta debe mantener actualizada una base de datos con intrusiones potencialmente peligrosas, criterios de transmisión para aceptar la información; y que mejor si a dicha estructura se puede adicionar herramientas de búsqueda

constante que sean actualizadas periódicamente, de modo que puedan convivir con antivirus, tomando en cuenta que para esto es necesario disponer de un ancho de banda adecuado, pero de no disponerlo, haya la posibilidad de integrar tecnologías para solucionar el problema de ataques de intrusos.

Para prevenir y contrarrestar una amplia gama de amenazas a las redes, es necesario conocer las características del tráfico e identificar los diversos tipos de ataques provenientes de instituciones externas.

El proyecto presentado a continuación proporciona el estudio de tecnologías de Prevención de Intrusos que conjuntamente se integran dentro de una red basándose en Redes Neuronales Artificiales destacando sus ventajas, desventajas, formas de obtención de entradas, pesos y funciones umbrales para su activación, sobre todo si esta información es proveniente de internet, pudiendo estar sometido a vigilancia, contando con monitoreo de los procesos a través del entrenamiento utilizando la gradiente de su función para establecer el menor error posible y con esto reconocer activamente el tráfico anormal.

1.4 Objetivos

1.4.1 Objetivo General

Analizar, un Sistema de Prevención de Intrusiones basada en modelos de redes neuronales recurrentes con características adaptativas de diferenciación y clasificación de datos que permitan utilizar una función umbral de activación a través del estudio de su

gradiente para aprendizaje entrenado con atributos de paquetes transmitidos; y diseñar una propuesta para la infraestructura de la Unidad Educativa Brethren.

1.4.2 Objetivos Específicos

- ✓ Identificar atributos de los protocolos más comunes en los paquetes de datos utilizados en la red, al momento de iniciar, durante y al finalizar la conexión, mediante herramientas de análisis de vulnerabilidades y ataques.
- ✓ Analizar las redes neuronales recurrentes con sus respectivas capas ocultas para; implementar la más adecuada que cumpla con la clasificación, prevención y bloqueo de tráfico peligroso que fluye por la red procurando utilizar la menor cantidad de atributos de paquetes para su aprendizaje.
- ✓ Analizar y evaluar un Sistema de Prevención de Intrusos que permita integrar su estructura con la Red Neuronal Artificial, y el número de neuronas necesarias para implementar la red adaptada.
- ✓ Definir un diseño de Red Neuronal Artificial, a través de sus atributos de paquetes como entradas receptadas en un Sistema de Prevención de Intrusos y adaptando su entrenamiento mediante el estudio de su gradiente para minimizar errores de pesos para la Unidad Educativa Brethren.

CAPÍTULO 2

ESTADO DEL ARTE

2.1 Seguridad Informática

Tomando en cuenta que la evolución de las comunicaciones dan pasos gigantescos, el mantener una revisión constante de la información transmitida permite controlar accesos de determinado tráfico a la red, por ello es de suma importancia conocer las características que estas mantienen al trasladarse de un punto a otro.

Para lograr un control efectivo de la transmisión de información se lo puede hacer a través de una planificación que permita el control del flujo de tráfico a través de políticas elaboradas por los administradores de la red tomando en cuenta que deben ser políticas flexibles que controlen la información pero a la vez que permitan a los usuarios cumplir con sus tareas sin perder la efectividad del trabajo.

El mantener una planificación para las redes controladas debe suponer que estas tendrían la posibilidad de desarrollarse, extendiéndose por varios puntos de la empresa con lo cual las políticas implementadas deben tomar en cuenta que siendo información de otros departamentos pueden iniciarse transmisión de información que no corresponda a la que regularmente suele utilizarse, en estos instantes muchos administradores implementan firewalls[1] con la intención de filtrar paquetes, sin embargo puede convertirse en un problema

[1] Firewall: Es software o hardware que captura información proveniente del internet o una red para comprobar su contenido, este puede bloquear o permitir el paso de esta información dependiendo de la configuración establecida.

ya que se restringe el acceso a varias aplicaciones o a la ves por ser políticas restrictivas podría interferir con direcciones de los otros puntos.

Ante lo mencionado se puede decir que para asegurar una red deben crearse políticas de seguridad que permitan a los administradores controlar el flujo de la información tomando en cuenta que estas deben ser en gran porcentaje transparentes para los usuarios sin olvidarse que al realizar este control podemos cometer errores sino hacemos evaluaciones de varios factores como son:

2.1.1 Evaluaciones de riesgo, *"La evaluación de la amenaza y los riesgos no debe ser una actividad de una sola vez; debe realizarse con regularidad, como se defina en la política de seguridad del sitio"* (ALVAREZ, 2005, p. 11). Estas evaluaciones son análisis de control de actividades realizadas en la red que puedan comprometer la transmisión o que deje abierto puntos en los cuales sean muy fáciles de interceptar para los atacantes, o a la vez, sean datos que pertenecen a la institución y que tengan altos índices de confidencialidad, sin embargo el nivel de seguridad no puede ser idéntico para todos los casos como por ejemplo: asegurar las bases de datos en las cuales lleguen noticias públicas no tendrá el mismo nivel que los datos personales de docentes y directivos, de igual manera se considera el costo beneficio ya que no es recomendable asegurar datos en los cuales el costo será mayor que el impacto de bienestar en la institución, se las realiza tomando en cuenta la importancia de la información y los riesgos que implica la manipulación de la misma, a los cuales se suele llamar peso siendo esta el producto del riesgo R por la importancia de los datos W, además debemos considerar el grado de disponibilidad de los recursos que manipulan la

información, la integridad al transmitir y su confidencialidad de ahí la importancia de analizar toda la información transmitida, para lo cual existen técnicas que permiten mantener la información clasificada de acuerdo a su grado de sensibilidad que a más de hacerla privada puede ocultar y disimular el tráfico transmitido aparentando datos no significativos para los atacantes.

2.1.2 Amenazas

En muchos casos la información transmitida es interceptada, falseada o regalada a personas que sacan provecho de esta ya sea dentro de la empresa o fuera de ella por diversos motivos que comprometen en si toda la estructura de funcionamiento. Como se observa en la Figura 1, a estas actividades se las conoce como amenazas las cuales se pueden presentar en forma interna o externa a la empresa, creada por seres humanos o por casos no controlables fácilmente como son los desastres naturales. Para este estudio es más importante el caso de amenazas creadas por seres humanos sean estas maliciosas o no ya que lo trascendental aquí es mantener un control de dichas amenazas las cuales en muchas veces suelen ser internas debido a que los empleados tienen acceso a la mayoría de dispositivos, claves, tráfico, etc., fácilmente dentro de la empresa y en muchas ocasiones por inconvenientes entre empleado y jefes la mejor manera de obtener beneficio saboteando su información. Las amenazas suelen desarrollarse como: virus informáticos con la intención de dañar las plataformas operativas aprovechándose de las vulnerabilidades de estas o con intención directamente de robo y si un empleado no tiene normas establecidas para el acceso a esta información la puede utilizar o a la ves entregar a personas externas, o en muchos

casos la ignorancia al aceptar cualquier indicio de mejorar su economía, indagar en redes sociales, pornografía o solo por ver propaganda provocan que los atacantes se apoderen de su computador fácilmente.

En ocasiones estas amenazas ni los propios administradores logran controlar ya que la abundancia de tráfico que fluye en la red es difícil analizarla en forma rápida, para esto la implementación de minería de datos[2], análisis forense de tráfico [3] o un análisis exhaustivo con las herramientas correspondientes puede ayudar a combatirlas.

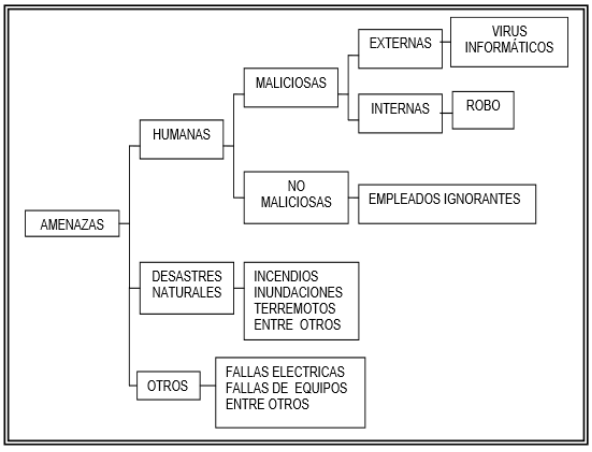


Figura 1. Tipos de amenazas en una empresa.

Fuente: (Hernandez, 2006, p. 44)

[2] Minería de datos: Procesos que buscan descubrir patrones en grandes volúmenes de datos buscando transformarlos en estructuras comprensibles.

[3] Análisis forense se tráfico: técnicas de reconstrucción de tráfico de red mediante las cuales se puede dar respuesta a un número de eventos generados en determinado tiempo para explicar el uso que se ha dado a los dispositivos informáticos.

2.1.3 Políticas de seguridad

Cuando en una institución se presentan desastres dentro de su red ya sean estos humanos (amenazas) o naturales lo primero que su administrador procura seguir para enfrentarlos, es una búsqueda de guías que le permita saber cómo está estructurada dicha red, sus niveles de seguridad, sus recursos utilizados, su organización con los integrantes del equipo, su infraestructura, etc., de no existir estas guías la probabilidad de colapso es muy alta. A estas se las conoce como Políticas de seguridad las cuales permiten seguir de forma planificada las decisiones a tomarse en caso de un desastre, estas permiten en la mayoría de los casos dar soluciones rápidas que admitan continuar con el trabajo correspondiente de la red, que en muchas ocasiones no puede bajo ninguna justificación detenerse como por ejemplo: las instituciones financieras o en el área de la salud.

Para realizar políticas de seguridad hay que tener en cuenta que todo el personal de la institución debe involucrarse en su elaboración, claro está que hay que dar a cada departamento su participación correspondiente ya que no todos pueden manejar los niveles de seguridad de la misma manera.

El documento de la Política de Seguridad de la Información debería enunciar el compromiso de la gerencia. En otras palabras, debería contener:

a) Una definición de la seguridad de la información, sus objetivos, alcances generales y la importancia.
b) La intención de la gerencia, sus objetivos y los principios de la Seguridad de la Información en línea con la estrategia y los objetivos comerciales.

c) Un marco referencial para establecer los objetivos de control y los controles incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo.
d) Una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad.
e) Una definición de las responsabilidades generales y específicas para la gestión de la Seguridad de la información incluyendo el reporte de incidentes de Seguridad de Información.
f) Referencias a la documentación que fundamenta la política; por ejemplo, políticas y procedimientos de seguridad más detallados para sistemas de información específicos o reglas de seguridad que los usuarios debieran observar y cumplir.

En los literales antes mencionados se indica lo que un documento de Seguridad Informática posiblemente debe contener como políticas, pero esto se realiza de acuerdo a un análisis entre el equipo y los directivos de la institución, ya que debe concordar a las necesidades y realidad de cada empresa como en este caso UNIPLEX SYSTEM S. A. (POSSO, 2009, p. 7).

El realizar Políticas para la Seguridad de la Información dentro de cualquier institución no se debe tomar a la ligera, se ha mencionado acerca de lo que podría contener en un inicio este documento, sin embargo se debe tener en cuenta que para desarrollar estas políticas dentro de cualquier empresa se dispone de: equipo de directivos, supervisores, empleados, proveedores, clientes, personales especializado para realizar pruebas de monitoreo de tráfico

y Ethical Hacking[4] interno como externo, etc., en lo que respecta al talento humano. Luego se debe tener en cuenta la infraestructura de la empresa como es el caso: departamentos, equipo eléctrico, computadores personales, servidores, equipos terminales, medios de comunicación estáticos y móviles, medios de transmisión, la comunicación a través de correo, redes sociales, acceso de los usuarios a las aplicaciones, etc., las políticas que se diseñen deben estar acorde a cada uno de los puntos señalados que se relacionen entre sí, todo determinado en un orden lógico que permita a cualquier administrador implementar nuevas tecnologías, aumentar equipos o utilizar software como es el caso de este estudio.

2.2 Protocolos de comunicación

2.2.1 Protocolos

Los protocolos son reglas establecidas y bien definidas que permiten la comunicación entre entidades de una red, tomando en cuenta que cada uno de estos tiene características específicas de acuerdo a la capa de red en la que se encuentre, intentando la comunicación, estas deben tener la capacidad de entenderse entre sí. Los protocolos de comunicación pueden ocupar las siete capas del modelo OSI o TCP/IP, o solo una parte de ellas, dependiendo la aplicación que se vaya a ejecutar. La mejor manera de enviar un mensaje es directamente, sin ninguna conversión entre el emisor y el receptor ya que con esto no se tendría problemas al transmitir, sin embargo por seguridad y reducir costos de recursos, es

[4] Técnicas previstas por una institución para explotar las vulnerabilidades existentes en un sistema objetivo valiéndose de un test de intrusión.

conveniente convertir los datos que se transmiten, quiere decir que estos no viajarán originalmente como el usuario los visualiza o como la aplicación que los gestiona, se establecen reglas para que se les permitan hablar un mismo idioma a los protocolos que intervienen en la comunicación, secuencias que al ser transferidos por diferentes dispositivos (gateways o routers) o capas según el modelo de red utilizado permitirán realizar la comunicación, y estos viajen en forma segura, se entiendan entre dispositivos y procuren perder datos lo menos posible, al enviarse convertidos estos desde un protocolo a otro, por ejemplo: el protocolo TCP es uno de los más utilizados en la transferencia de información, se encuentra en la capa de red y este es orientado a la conexión, esto quiere decir que necesita realizar un three-way handshake (Chayan, 2009, p. 3, 4) para iniciar, la información viaja desde la capa de aplicación hasta la capa de transporte dependiendo de la (multiplexación de conexiones) utilizada, por ejemplo para enviar un correo es necesario el puerto 25, para posteriormente en la capa de transporte obtener con el protocolo TCP una cabecera (encapsulación) Figura 2, continuando su camino a la próxima capa, considerando que los datos pudieron ser fragmentados para lo cual las cabeceras serán para cada fragmento.

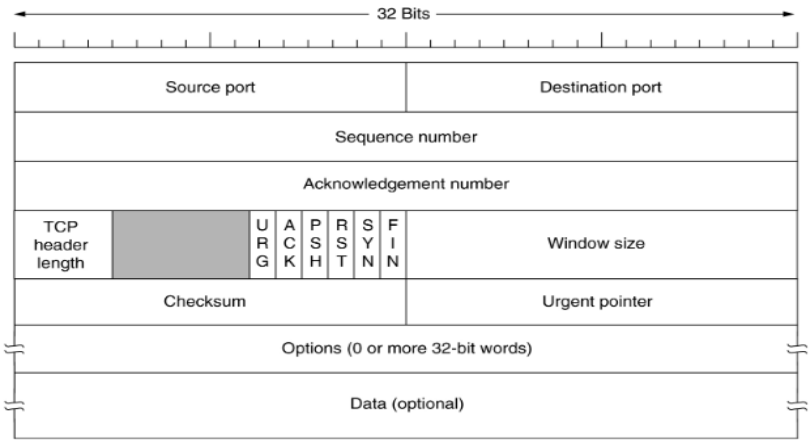


Figura 2. Cabecera TCP

Fuente: (Naranjo, 2013)

Hoy en el ámbito de las comunicaciones en subestaciones, todos los protocolos puede ser recibidos a través de convertidores de protocolos, pese a esto se pueden producir errores en el mensaje e introducir retrasos o perdida en la entrega de datos, de ahí la importancia del análisis de su funcionamiento, características, tipos de protocolos, para encontrar soluciones a irregularidades al momento de analizar el tráfico que fluye por la red mediante estos. La gran cantidad de protocolos hacen que el desarrollo tecnológico tenga que crecer, en especial los fabricantes y aumentan los costos de operación y de mantenimiento, este crecimiento necesita de un control en la transferencia de datos con la finalidad de localizar ataques en momentos oportunos.

Dos equipos de diferentes marcas se pueden comunicar solo si usan el mismo protocolo, es por ello que hay una gran cantidad; los cuales pueden dividirse en dos categorías:

2.2.1.1 Protocolos Propietarios siendo estos creados por una empresa con fines específicos que solo funcionarán con los dispositivos que les pertenecen, pueden estos utilizar las capas del modelo OSI o del modelo TCP/IP Figura 3, (siendo estos modelos de capas libres) dando características de comunicación para direccionamiento e identificación del destino a los paquetes de datos en el caso de la capa de transporte. Si un dispositivo no cuenta con esos protocolos la comunicación no podrá realizarse ya que se puede decir que están hablando distintos idiomas y no hay compatibilidad, es por ello que no solo es un protocolo de comunicación el que interviene, sino una pila entera de protocolos los cuales actúan durante toda la comunicación: El protocolo IPX/SPX es un ejemplo de protocolos propietarios pertenecientes a Novell desarrollado para la arquitectura Netware, otro de los principales fabricantes de protocolos propietarios suele ser CISCO SYSTEMS[5], este, fabrica los protocolos en la mayoría para enrutamiento entre los dispositivos de su propiedad, al comprar por ejemplo un router diferente al de marca CISCO puede este realizar una comunicación con protocolos estándar como es el caso de RIP[6] pero si se desea un protocolo más robusto entre los routers por ejemplo EIGRP[7] la comunicación se detiene puesto que el dispositivo CISCO los podrá identificar pero el dispositivo estándar no.

[5] Es una empresa con sede en San José (Estados Unidos) distribuida a nivel mundial, dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.
[6] Protocolo de puerta de enlace interna utilizado por los routers para intercambiar información acerca de las redes que se encuentran conectadas.
[7] Es un protocolo de enrutamiento vector distancia que ofrece algoritmos vector distancia y estado de enlace.

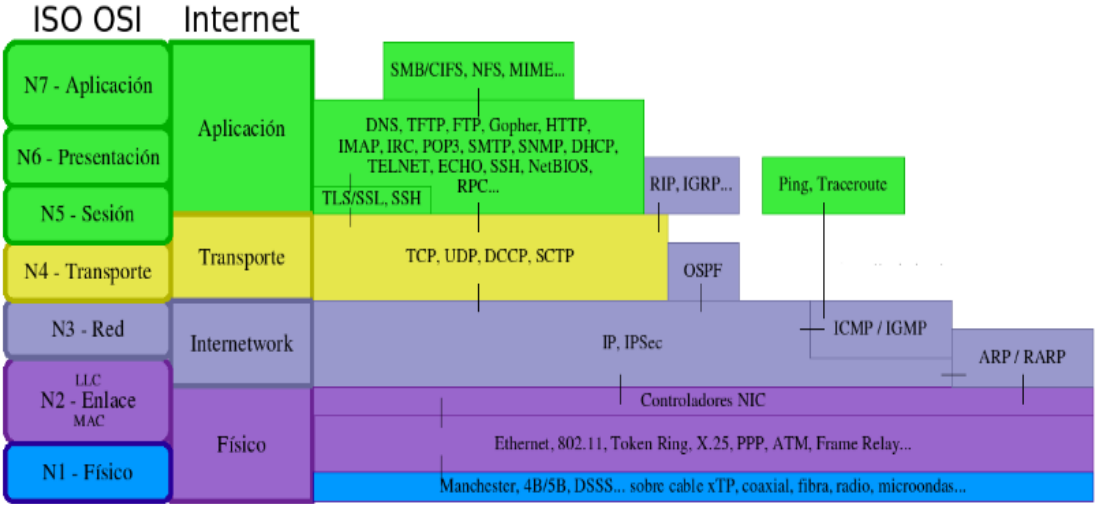


Figura 3. Capas del modelo OSI y TCP/IP con subcapas.

Fuente: (Guimi, 2009, p. 14)

2.2.1.2 Protocolos Abiertos, se caracterizan porque no tienen ninguna licencia o patente que limite su utilización, manipulación o modificación, en gran parte de las redes son manipulados como estándares a nivel mundial públicamente conocidos como es el caso del internet (monografías.com, 2014) y que tienen compatibilidad con otros protocolos, en algunos casos fueron elaborados inicialmente con patentes de sus creadores pero a medida que eran necesarios para la comunicación y la gran cantidad de información que se suponía para la transmisión era a cada momento tipo full-dúplex los administradores se encontraban con diversos problemas, uno de los más comunes, las colisiones, para estos casos era necesario la experiencia de usuarios en los que se manifieste necesidades y corrección de errores con lo que provocó por la gran demanda a medida que los computadores llegaban a los hogares, que la estructura de los protocolos sean administrados por los usuarios llevando

a ser estandarizados por empresas que disponen del estudio técnico correspondiente para su utilización como es el caso de IEEE, IETF, ITU-T entre otras.

Los elementos básicos de un protocolo de comunicaciones son: un conjunto de símbolos llamados conjunto de caracteres, un conjunto de reglas para la secuencia y sincronización de los mensajes construidos a partir del conjunto de caracteres y los procedimientos para determinar cuándo ha ocurrido un error en la transmisión y como corregir el error. El conjunto de caracteres se formará de un subconjunto con significado para las personas (usualmente denominado como caracteres imprimibles) y otro subconjunto que transmite información de control (usualmente denominado caracteres de control). Hay una correspondencia entre cada carácter y los grupos de símbolos usados en el canal de transmisión, que es determinado por el código. Muchos códigos estándar con sus respectivas equivalencias de grupos de unos y ceros (bits) han sido definidos con el paso de los años. El conjunto de reglas a seguir por el emisor y el receptor propicia: que haya un significado con secuencias permitidas y a tiempo, entre los caracteres de control y los mensajes formados a partir de los símbolos. La detección de error y los procedimientos de corrección permiten la detección y la recuperación ordenada de los errores causados por factores fuera del control de la terminal en cada extremo, al querer interpretar el flujo de la información en un canal se debe conocer a profundidad los elementos de un protocolo de comunicación.

Para que exista comunicación en ambos puntos al extremo de un canal se deben emplear la misma configuración de protocolos. (Romero, 2006)

Los protocolos gestionan dos niveles de comunicación distintos. Las reglas de alto nivel definen como se comunican las aplicaciones, mientras que las de bajo nivel definen como se transmiten las señales. El protocolo de bajo nivel es básicamente la forma en que las señales se transmiten, transportando tanto datos como información y los procedimientos de control de uso del medio por los diferentes nodos. Los protocolos de bajo nivel más utilizados son: Ethernet, Token ring, Token bus, FDDI, CDDI, HDLC, Frame Relay y ATM.

Una breve descripción de los protocolos de bajo y alto nivel más utilizados permite en este documento avizorar sus características y utilización para enfocarse hacia qué tipo de tráfico controlar al momento de realizar la transmisión de paquetes en una comunicación procurando identificar intrusiones:

2.2.2.1 Ethernet

Este protocolo aparece a partir del diseño de redes LAN por los años 70 que en su común al transmitir presentaba la gran desventaja de las colisiones: al enviarse determinada información se esperaba una respuesta de haber recibido los paquetes enviados, al no recibirla se reenviaba nuevamente sin tomar en cuenta que pudo haber colisionado por algún punto de la red, esto en caso de que la transmisión fuese de dos estaciones, es de imaginarse la saturación a gran escala al ser utilizado el canal para transmitir varias estaciones en forma simultánea, debido a esto se crea el protocolo CSMA/CD (Acceso Múltiple con Detección de Portadora y Detección de Colisiones) en topologías como: anillo, estrella o bus, y a través de DIX (Digital Equipmen Corporation, Intel and Xerox) se crea el comité 802 con el servicio de datagramas con el mejor esfuerzo siendo este simple y flexible el cual acepta a

Ethernet por medio de IEEE como 802.3 esta dispone de dos mejoras esenciales al transmitir la información; la primera indica que si una estación está hablando otra no puede transmitir, y la segunda es que si se produce una colisión las estaciones se callan mediante un algoritmo (backoff) reduciendo la probabilidad de colisiones, en lugar de seguir transmitiendo se planea la retransmisión durante un tiempo aleatorio, mientras tanto se envía una señal Jam para saber si el canal está desocupado, pero si una estación encuentra que el medio esta ocioso procede a realizar la transmisión, quiere decir que si una estación comienza la transmisión en un determinado tiempo se procura que la otra no comience en ese instante.

A medida que el tráfico aumenta en el canal, existe una probabilidad mayor de colisiones, para esto Ethernet utiliza el Retroceso Exponencial Binario tomando en cuenta que este es auto-adaptativo procurando evitar la duplicación en el tiempo de reenvíos que realiza el backoff a partir de la colisión 10 llegando esta hasta la 16 en la que detiene el envío y el protocolo MAC descarta la trama y reporta fallo a nivel de red.

Dadas estas particularidades Ethernet es uno de los protocolos más utilizado en la mayoría de las transmisiones desde su aparición hasta su desarrollo completo Figura 4, tomando en cuenta que los subcomités 802 fueron incrementando velocidades, varías tecnologías buscan la forma de hacerle competencia la FDDI sin tener mucho peso en el mercado por su poca alternativa de compatibilidad con Ethernet, por su por su gestión compleja y precios inaccesibles, la ya inexistente ATM que era utilizada en el núcleo del sistema telefónico lo cual difiere de Ethernet que trabaja con LAN en su mayoría, que en algún momento aspiró funcionar a las mayores velocidades pero con unos precios elevados,

o la ya extinta Token Ring, sin embargo por ser un protocolo que puede utilizar altas velocidades llegando hasta el usuario final se complica su alcance puesto que casi un 85% en 1985 de las conexiones de red eran Ethernet más aún en la actualidad, tomando en cuenta que se mejoró la velocidad a la que ahora conocemos como Gigabit Ethernet.

A pesar de la eficiencia de Ethernet en un canal se puede decir que si una trama es pequeña con relación a una velocidad grande puede haber saturación, con lo cual debe existir tramas mínimas más grandes en velocidades altas a distancias igualmente grandes, sin embargo aún existe el riesgo de colisiones, por lo cual esto se puede solucionar a través de Ethernet conmutada mediante un switch ya que sus tarjetas para conmutación son independientes entre sí en la transmisión, se supone que el CSMA/CD actúa de igual manera pero con la diferencia que por cada conector funcionaría independientemente lo que no se puede lograr solamente en un solo canal sin conmutador, de ahí que este dispone de un BÚFFER (memoria RAM) que puede almacenar las tramas para luego enviarlas a su destino correspondiente.

1970	Primeras experiencias de redes broadcast en Hawaii: ALOHANET. Protocolos MAC: ALOHA puro y Ranurado.
22/5/1973	Robert Metcalfe y David Boggs conectan dos ordenadores Alto con cable coaxial a 2,94 Mbps en el *Xerox Palo Alto Research Center*, mediante una red denominada Ethernet.
Mayo 1975	Metcalfe y Boggs escriben un artículo en el que describen a Ethernet, y lo envían para su publicación a *Communications of the ACM*.
1976	*Xerox* crea SSD, una división para el desarrollo de los ordenadores personales y la red X-wire (nuevo nombre de Ethernet).
1979	Se constituye la alianza *DIX* (DEC-Intel-Xerox) para impulsar el desarrollo técnico y comercial de la red. Se vuelve al nombre original de Ethernet. Metcalfe abandona *Xerox* y crea *3Com*.
Febrero 1980	El IEEE crea el proyecto 802.
Abril 1980	*DIX* anuncia al IEEE 802 que está desarrollando una tecnología de red local que pretende estandarizar.
Septiembre 1980	*DIX* publica Ethernet (libro azul) versión 1.0. Velocidad 10 Mbps.
1982	*DIX* publica Ethernet (libro azul) versión 2.0. *3Com* produce las primeras tarjetas 10BASE2 para PC.
24/6/1983	IEEE aprueba el estándar 802.3, que coincide casi completamente con DIX Ethernet. El único medio físico soportado es 10BASE5.
1/1/1984	*AT&T* se subdivide en *AT&T Long Lines* y *23 BOCs (Bell Operating Companies)*. Los tendidos de cable telefónico internos de los edificios pasan a ser gestionados por los usuarios.
1984	*DEC* comercializa los primeros puentes transparentes
21/12/1984	*ANSI*[4] aprueba el estándar IEEE 802.3.

Figura 4. Cronología de Ethernet hasta ser aprobado como estándar

Fuente: (Marquéz, Pardo, & Pizarro, 2001)

Posteriormente se conoce que a cada momento aumentan las estaciones y las redes incrementando de igual manera el tráfico en un canal reduciendo el ancho de banda puesto que se encuentra en un rango de frecuencias limitado, a esto se propone la Fast Ethernet(802.3u) que es un agregado al estándar 802.3 reduciendo el tiempo de bits de 100ns a 10ns manteniendo la misma arquitectura del 802.3 para mantener la compatibilidad con las tecnologías anteriores, la diferencia es que se reduce la longitud del cable y no se permite conexiones múltiples con derivaciones. Para lograr el cambio se utiliza un tipo de cableado 100BaseTX2 en cables de categoría 3 con codificación 4B/5B pero se necesitó un procesador de señales sofisticado lo cual aumenta su precio considerablemente.

La velocidad de transmisión se incrementó notablemente con Fast Ethernet, sin embargo el IEEE quiere aumentar la velocidad por lo que aparece gigabit Ethernet (802.3z), funciona a base de semiduplex pero en conexiones a concentradores en la cual utiliza el protocolo CSMA/CD estándar, en dúplex total no importa el envío de la trama por parte del computador o el conmutador al mismo tiempo sin necesidad de detectar si el canal está en uso, desaparece el protocolo CSMA/CD, continua con la autodetección de velocidad, la longitud del medio de transmisión depende de la fuerza de la señal, a estas velocidades 100 veces mayores que 802.3 y con tramas de 64 bytes se reduce la longitud del cable a 25 metros, se aumenta el ancho de banda a 512bytes, en cuanto a software en la carga útil se trabaja por relleno si no es completa la trama, la eficiencia del canal se reduce a un 9%, no obstante por la característica de ráfaga de tramas permite que un emisor transmita una secuencia concatenada de múltiples tramas en una sola transmisión siendo muy eficiente como esquema de transmisión ampliando el radio de la red a 200 metros, y manteniendo la compatibilidad hacia atrás pero con el problema del costo en hardware.

La velocidad aumenta a casi 1Gbps, en fibra óptica con características propias la velocidad con código Manchester pero con una señal de 2 Gbaudios difíciles de conseguir por lo que se opta por codificación 8B/10B siendo así satisfactoria pero con competencia de menores costos con UTP, esto es un problema ya que si la velocidad de la fibra óptica es muy alta a diferencia del dispositivo que recibe la información puede saturar el BUFFER de este a lo cual se utiliza el control de flujo como lo hace Fast Ethernet pero siempre buscando mayores velocidades. (Tunembaum, 2003)

2.2.2.2 Token ring

IEEE 802.5 fue creada y muy utilizada en tecnología LAN después de Ethernet casi por las mismas fechas en lo que refiere a popularidad, utiliza como topología un anillo físico y lógico que permite el flujo de los datos en un solo sentido, como protocolo de acceso al medio utiliza el Token passing con el cual determina que nodo quiere transmitir, este anillo tiene varios nodos conectados, cada nodo recibe frames del nodo que le antecede para luego enviar al nodo que sigue, solo un nodo puede transmitir frames mientras tiene el token durante determinado tiempo THT (token holding time) para luego de la transmisión liberar el token, el resto de nodos no puede transmitir para evitar colisiones, el token es un patrón especial de y 3 bytes (24 bits) y un campo de tres bits con niveles de prioridad para la solicitud del token que viaja sobre la red en forma libre pasando por cada nodo hasta que alguno de estos quiere transmitir, al obtener un nodo el token, envía en su lugar el frame con la información que desea transmitir, el receptor hace una copia del mismo y el frame continua en la red hasta ser retirado por el emisor, el mismo que sabe exactamente si el frame fue visto y si tuvo alguna copia.

En Token Ring es posible calcular exactamente el tiempo en dar la vuelta el token al anillo ya que es determinista con lo cual se puede saber exactamente los tiempos a manejarse para las respectivas transmisiones. "El protocolo 802.5 dispone de una forma confiable de entrega de frames a través de dos bits llamados A(ARI) y C(FCI) los cuales al iniciar el trabajo de la red tienen el valor de cero;

- Cuando un nodo ve un frame que es para él, coloca el bit A en 1 (uno).

- Cuando hace copia del frame coloca en 1 (uno) el bit C.
- Si la estación transmisora ve regresar el frame con el bit A aún en 0 (cero), sabrá que el nodo destino no está o está funcionado mal. Si el bit A está en 1 (uno) pero el bit C está en 0 (cero), por alguna razón (por ejemplo, buffers del adaptador llenos) el nodo destino no pudo aceptar el frame. Esto permite retransmitir el frame posteriormente, cuando el buffer esté más desocupado". (net, 2002, p.14)

2.2.2.3 Token bus

Este protocolo fue presentado por la IEEE con el número 802.4, de características físicas similares a la Ethernet en bus con cable coaxial pero con normas totalmente incompatibles y de características lógicas similares a Token Ring con paso de testigo. Los nodos que son asociados en un anillo dentro de la topología bus cumplen con la transmisión en un solo sentido (univoca) cada estación tiene un número asociado con el cual se puede identificar en la red, el que tiene el número mayor es que inicia la transmisión y este conoce a su vecino antes y después de la recepción y envío de la trama. Figura 5, este protocolo fue desplazado por el gran uso de Ethernet ya que su sistema probabilístico de resolución de colisiones provoca retardos importantes en la cual ciertas aplicaciones no los soportan, adicionando a esto que el cableado de la red en forma longitudinal es más sencillo de instalar que el circular y muchas redes ya disponían topologías bus por lo que fue necesario asociar nodos en forma lógica para aprovechar la infraestructura existente, la gran ventaja de este protocolo es que solo puede transmitir el nodo que tiene el testigo, igual que Token Ring evitando en gran parte las colisiones, sin embargo hay que tomar en cuenta que todos los nodos tienen acceso

al frame que se está transmitiendo funcionando como un repetidor, la incorporación o desconexión de un nodo a la red se loa hace a través del protocolo MAC sin existir interrupción en el paso de testigo, el protocolo token bus opera en la capa de enlace con la subcapa LLC y MAC. (Kaneria, 2012)

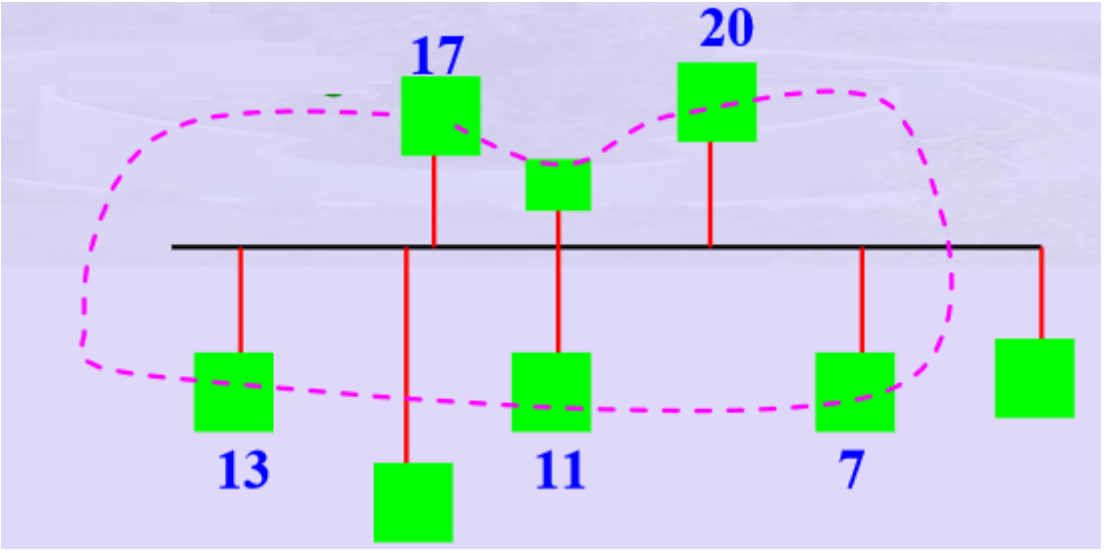


Figura 5: Esquema lógico de protocolo Token Bus

Fuente: (Murthy, 2015)

2.2.2.4 F.D.D.I

Es un protocolo con características de tramas similares a Token Ring utilizando el paso de testigo pero con grandes diferencias en velocidad de 100 Mbps y estructura de autoencabezamiento en caso de sufrir errores las estaciones pueden identificarlos y tomar medidas (tolerancia a fallas), todo esto basado en fibra óptica multimodo y utilizando codificación 4B/5B porque si se utilizaría codificación Manchester tendría que utilizar

200Mbaudios lo que se considera costoso, sin embargo se puede salvar el ancho de banda penalizando la autosincronización de reloj pero pudiéndose corregir por medio de preámbulos largos en las tramas enviadas, el objetivo principal de este protocolo es la alta velocidad de transmisión y la conexión entre redes individuales a altas velocidades. Este protocolo está diseñando para gestionar desde redes locales especializadas hasta redes troncales por su seguridad y confiabilidad con tramas de hasta 4500 bytes, por ejemplo en una red especializada, utiliza principalmente estaciones en una conexión (SAS), en doble conexión (DAS) y concentradores de doble conexión (DAC) todo esto lo puede realizar en un anillo o doble anillo, en el caso de que un anillo deje de funcionar esta recurre al otro anillo mientras las estaciones dan solución al daño y sus causas a través de una interruptor óptico, tomando en cuenta que un protocolo FDDI maneja transmisión con longitudes ilimitadas o se puede transmitir varias tramas en forma simultánea a diferencia de Token Ring, el testigo del protocolo MAC de FDDI maneja dialogo multipaquete.

Se puede decir que protocolo FDDI funciona como un enlace backbone Figura 6., para redes de alta velocidad, en un anillo su longitud es de 200km y con 2 anillos de 100km en los dos casos con casi 500 estaciones conectadas por anillo transmitiendo en sentidos contrarios, a medida que los datos a transmitirse aumentan su tamaño como es el caso de multimedia en tiempo real la velocidad debe aumentar dejando de lado el doble anillo para reducir costos. Se ha mencionado acerca de la fiabilidad, sin embargo el aumento de la demanda de usuarios a la red provoca una desmesurada saturación lo cual determinaría que la fiabilidad tiene sus límites y al tener una leve interrupción todos los usuarios tendrían una

importante ruptura, lo cual en cuanto a capacidad contradice su ventaja de fiabilidad saturándose al aumentar usuarios, sin embargo su alta tasa de operación de 8 a 10 veces las redes convencionales llama la atención para la conexión de redes de baja velocidad con minicomputadoras y mainframes siendo en este caso FDDI la red troncal, también hace uso de las ventajas de la fibra óptica en cuanto a velocidad, capacidad, inmunidad a interferencias y lo que le caracteriza más, la dificultad de pinchar un conductor de luz.

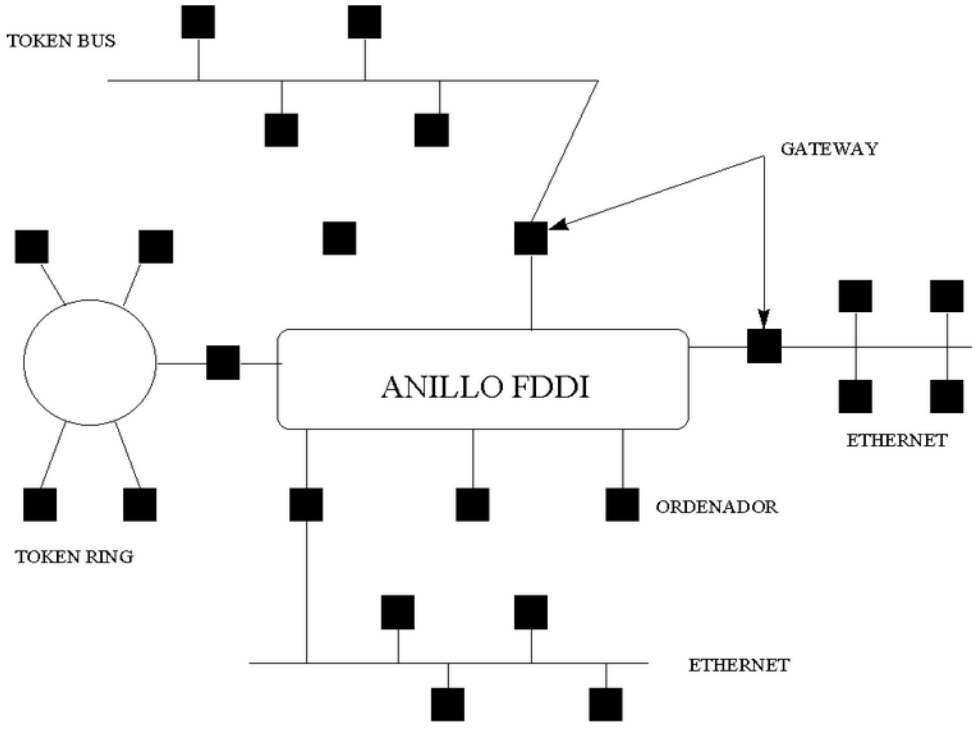


Figura 6: Diseño y conexión de una red con protocolo FDDI

Fuente: (Alba, 2005 - 2013)

El protocolo FDDI dispone de un subgrupo de especificaciones:

2.2.2.4.1 MAC. Formato de la trama, direccionamiento, CRC y mecanismos de recuperación de errores.

2.2.2.4.2 PHY. Procedimientos de codificación/decodificación, manejo del token, requerimientos de temporización y el entramado.

2.2.2.4.3 SMT. Configuración y características del control del anillo, conexión y desconexión de estaciones, control de fallas, programación y reunión de estadísticas.

2.2.2.4.3 PMD. Definición de las características del medio de transmisión.

Las especificaciones presentadas respecto a FDDI disponen de transmisión de datos con características similares a los protocolos citados anteriormente lo que significa que en el estudio de intrusiones en transmisión óptica es importante tomar en cuenta atributos de la información a para el análisis. (Sacanamboy, 2013)

2.2.2.5 C.D.DI.

Este protocolo fue diseñado con la idea de transmitir datos en cobre a velocidades de 100Mbps pero siendo una modificación al protocolo FDDI con cable de cobre de alta calidad.

Para cualquier PYME (pequeña y mediana empresa) la utilización de cobre representa disminuir costos en comparación con la fibra óptica tanto en cable como en instalación y terminaciones, tomando en cuenta que permite la transmisión de los datos de igual manera

que en otros protocolos pero a distancias relativamente cortas mediante la arquitectura de doble anillo para brindar redundancia. (Vaca, 2011)

2.2.2.6 H.D.L.C.

Este protocolo está orientado a la segunda capa del modelo OSI, con mecanismos para controlar enlaces digitales de datos punto a punto y multipunto incluyendo detección, corrección y recuperación de anomalías, su uso está basado en RDSI y X.25(no apto para tráfico en tiempo real y actualmente está obsoleto) pero la mayor parte con sus protocolos derivados ya que este es muy extenso, por medio de HDLC se puede definir qué tipos de estaciones se utilizan, como configurar los enlaces y los modos de operación en la transferencia de información, a continuación se describe las definiciones de HDLC:

2.2.2.6.1 Estaciones:

- Estación primaria: es la encargada de controlar el funcionamiento del enlace, siendo sus tramas llamadas órdenes.
- Estación secundaria: funciona bajo el control de las estaciones primarias por medio de enlaces lógicos y sus tramas generadas se denominan respuestas.
- Estación combinada: compuesta por características de las primarias y las secundarias, pudiendo generar tanto órdenes como respuestas.

2.2.2.6.2 Configuraciones de enlace:

- Configuración no balanceada: Se forma a través de una estación primaria y una o más secundarias, pudiendo utilizar transmisión full-dúplex y semi-duplex
- Configuración balanceada: transmisión de dos estaciones combinadas utilizando de igual manera transmisión full-duplex y semi-duplex.

2.2.2.6.3 Modos de transferencia de los datos:

- Modo de respuesta normal (NMR): Su utilización se la hace en configuraciones no balanceadas, la estación primaria inicia transmisión de datos hacia la secundaría como órdenes pero la secundaria solo lo puede hacer como respuestas, su uso se da en líneas con múltiples conexiones y con varios terminales conectados a un computador central la cual sondea las entradas de cada uno de los terminales.
- Modo balanceado asíncrono (ABM): Se utiliza en configuración balanceada, cualquier estación combinada puede iniciar la transmisión sin necesitar el permiso de otra estación combinada, este modo es el más utilizados de los tres ya que sus modos full dúplex son eficientes al no ser necesario los sondeos.
- Modo de respuesta asíncrono (ARM): Su uso se lo hace en la configuración no balanceada, la estación secundaria inicia la transmisión sin pedir permiso de la primaria.

2.2.2.6.4 Estructura de HDLC

La transmisión la realiza en forma síncrona entre el transmisor y el receptor, mediante el intercambio de tramas entre dos estaciones con un único formato, en cada trama dispone de campos de delimitación en los extremos con la combinación de bits 01111110.

2.2.2.6.5 Modos de operación de transferencia de datos

Al realizar un intercambio de información con HDLC se toma en cuenta la forma de operar esta transferencia lo que permite entender su funcionamiento:

- Iniciación: Es el modo en el cual una estación inicia una transferencia nueva o realiza un regeneración de una recibida, especificando cuál de los tres modos se está solicitando (NMR, ABM, ARM) con su secuencia de 3 o 7 bits, si la solicitud es aceptada, se recibirá una trama de confirmación en caso contrario se envía una trama de modo desconectado.
- Transferencia de datos: Una vez establecida la conexión lógica, ambos estaciones comienzan a enviar datos mediante tramas-I comenzando con el número de secuencia 0, dependiendo del modo de transferencia que esta utilice
- Desconexión: Al momento de cerrar la conexión, cualquiera de las dos estaciones puede realizar esta solicitud, ya sea por errores o por iniciativa propia, la estación que recibe la desconexión puede indicar si acepta o no devolviendo una trama UA (unnumbered acknowledged) informando a la capa superior acerca de la desconexión

la cual será responsable de recuperar tramas-I pendientes de confirmarse. (Calizaya, 2014)

2.2.2.7 FRAME RELAY

Es un protocolo de la capa de enlace de datos que funciona a través de la conmutación de paquetes WAN y conexión multiprotocolo de LANs, su servicio es orientado a la conexión compartiendo circuitos virtuales permanentes (PVC) por lo cual se alquila línea para realizar las conexiones T1 y circuitos virtuales conmutados (SVC), el costo es de acuerdo al uso; es una versión mejorada de X.25 y con eficiencia renovada en cuanto a velocidades altas (hasta 44.476Mbps) con un alto throughput y bajo retardo igual que las líneas T-3. El funcionamiento de Frame Relay lo hace a base de las dos primeras capas del modelo OSI reduciendo el retardo debido al procesamiento de cada trama que X.25 realizaba en la capa de transporte, el control de la transmisión lo realiza entre las estaciones finales, no entre los nodos intermedios lo que permite aumentar la velocidad, la corrección de errores depende de la capa de nivel 3 el mismo que tiene la posibilidad de realizar retransmisión lo que evita la sobrecarga en la capa física y de enlace.

La estructura de Frame Relay permite datos a ráfagas, esto quiere decir que puede en determinados momentos aumentar su velocidad y a momentos permanecer sin transmitir, con lo que requiere ancho de banda bajo demanda, por esto puede ser utilizada como una red troncal y su costo la hace más llamativa. Una característica principal de este protocolo es que permite tramas de longitud variable sin embargo puede tomarse como desventaja puesto que genera retardos variables a diferentes usuarios, las consecuencias se pueden observar al

enviar datos sensibles al retardo como video y audio en tiempo real, quiere decir, inadecuada para videoconferencias.

Las conexiones pueden ser DTE o DCE de acuerdo al dispositivo a conectarse, por ejemplo; un router al conectarse con una WAN y a la vez con varias LAN este dispositivo sirve como DTE, y el conmutador Frame Relay conectado servirá como un DCE, no es necesario el uso de direcciones físicas para definir el DTE sino el identificador de circuito virtual de conexión de enlace de datos (DLCI).

Las conexiones WAN – LAN mediante Frame Relay son métodos de red pública Figura 7, con una única línea dedicada en la cual se pueden poner varios circuitos virtuales sin provocar gastos elevados y un router asociado dentro de dicha red, siendo los paquetes de varios usuarios multiplexados sobre la línea y enviados a sus destinos con velocidades que fluctúan entre 64 Kbps y 2 Mbps apuntando a 35–45 Mbps en el futuro, debido a esto se permite que el control de errores sea desplazado a los equipos situados a los extremos de la comunicación con lo cual el transporte de los datos de un usuario a otro queda asegurado.

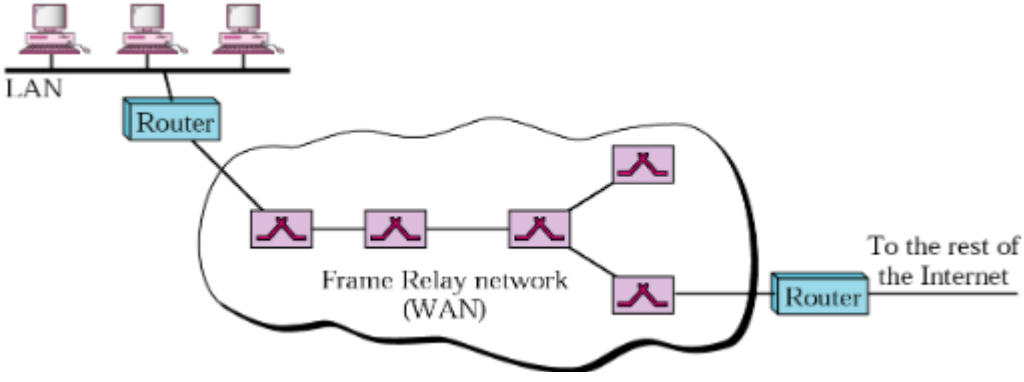


Figura 7: Estructura de Frame Relay
Fuente: (Villegas, 2005 - 2006)

Cuando se incrementa el volumen de la transmisión en forma considerable Frame Relay utiliza dos métodos para identificar la congestión y solicitar que se reduzca temporalmente la transmisión de datos: El primero lo realiza a través de las tramas BECN (Backward Explicit Congestion Notificación), FECN (Forward Explicit Congestion Notificación) y CLLM (Consolidated Link Layer Management), en algunos casos la respuesta es opcional y muy pocas veces es implementada, la mejor manera para evitar la congestión en la red es a través del descarte de datos. La segunda opción es a través del protocolo de nivel superior para identificar la retransmisión durante la carga de grandes tráficos. (Justicia, 2006)

2.2.2.8 A.T.M.

Por la década de los 90, a medida que se adhieren más dispositivos en las redes, la gran demanda de capacidad de transmisión para servicios y aplicaciones públicas provoca que las infraestructuras se adapten a mayores velocidades aumentando ancho de banda y conmutación a las redes troncales.

ITU-T desarrolla ATM (Asynchronous Transfer Model) siendo una arquitectura de protocolos diferente a la OSI y TCP/IP, se crea con la idea de; optimizar el uso de los medios de transmisión de alta velocidad y que sea un protocolo con capacidad de entregar datos seguros y un bajo costo. Los enlaces de equipos LAN no son directamente operativos en la WAN debido a las distancias con lo que ATM basándose en enlaces SONET logra realizar la transmisión con retardos insignificantes en comparación con la cantidad de información transmitida extremo a extremo, este protocolo funciona a base de celdas con unidades de 53 bytes dentro de las cuales se incluye información respecto a la conexión que pertenecen,

simplificando el hardware y los procesos en los nodos, reduciendo el tamaño de los buffers internos en los conmutadores y su gestión más rápida y eficiente, las celdas de transmisión se pueden reducir de tamaño y al ser iguales se reduce la variación en el retardo, la transferencia se lleva a trozos con lo cual puede ser multiplexada sobre una misma interfaz física, combina multiplexación de circuitos y paquetes, sin embargo si llegara a congestionarse puede descartar celdas aun siendo estas protegidas (se garantiza el enrutamiento), los direccionamientos de conexiones se realizan a través de canales virtuales (VCC), los sistemas finales entre sistemas y conmutadores o entre dos conmutadores los conecta a través de caminos de transmisión (TP), las conexiones entre dos conmutadores los realiza mediante camino virtual (VP), todas las celdas que pertenecen a un mismo mensaje viajan por un mismo circuito virtual (VC) manteniendo su orden hasta llegar al destino fijado, varios circuitos virtuales forman un camino virtual y la concatenación de varios caminos virtuales forman una conexión de camino virtual.

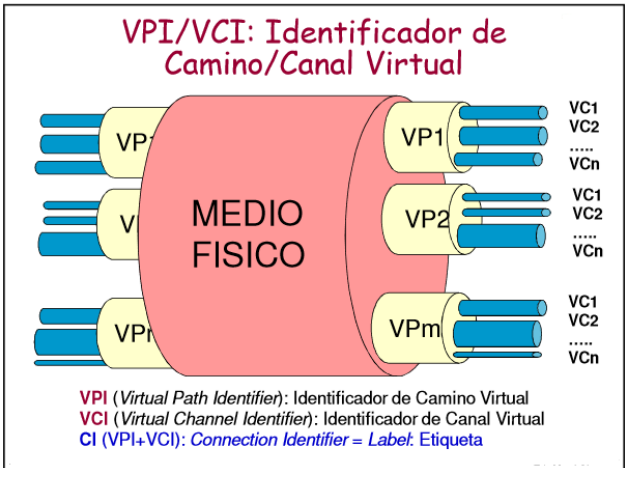


Figura 8: Estructura del protocolo ATM sobre un canal físico
Fuente: (Gallón, mayo)

El hecho que este protocolo se base en celdas a través de caminos virtuales rápidos Figura 8, repercute en un mejor aprovechamiento de la conmutación minimizando el coste de la transmisión y el procesamiento interno de la red, está orientado a la conexión pero no proporciona acuses de recibo gracias a esto las velocidades de transferencia van desde 25.6 Mbps a 622.08 Mbps, sin embargo esta rapidez induce que la transmisión sea asíncrona o estadística de acuerdo al volumen de la información provocando que no se pueda controlar fácilmente el tráfico para distintos tipos de servicio (QoS) lo que ha repercutido en que otros protocolos lo reemplacen. (Gallón, mayo)

El protocolo de red determina el modo y organización de la información (tanto los datos como los controles) para su transmisión por el medio físico con el protocolo de alto nivel. Los protocolos de red más comunes son: IPX/SPX, DECnet, X.25, TCP/IP, AppleTalk y NetBEUI.

2.2.2.9 IPX/SPX

Protocolo de características estrictamente privativas, creado por Novell diseñado para transmitir paquetes dentro de una red, su funcionamiento óptimo es específicamente en las redes locales LAN superando inclusive al protocolo TCP/IP, en las cuales demuestra el mejor funcionamiento por ser rápido, fácil de configurar y que requiere pocas atenciones, IPX funciona en la topología bus enviando datos mientras que SPX realiza la confirmación de los datos al llegar a su destino, el cual es utilizado en la topología anillo, en el modelo OSI trabaja en la 3ra capa (red) y 4ta capa (transporte), empaquetando y confirmando la llegada correcta del paquete incluyendo su integridad.

IPX es un protocolo de datagramas está orientado a comunicación de paquetes sin conexión, es muy similar a IP de TCP/IP en cuanto a sus operaciones básicas, pero difiere totalmente en cuanto a direccionamiento y formato de los paquetes, por otro lado SPX es muy fiable en cuanto a integridad de paquetes, actúa sobre IPX ya que, solo, no puede funcionar, de igual forma muy similar a TCP, se utiliza para aplicaciones cliente/servidor.

2.2.2.9.1 Estructura de la cabecera de paquetes

Está compuesta por 12 bytes conectados sobre una cabecera IPX de 30 bytes distribuidos Figura 9, de los cuales contiene todas las estructuras de SPX que utiliza para iniciar y mantener la conexión garantizando el envío de los datos en secuencia, junto con los datos y la cabecera, no pueden sobrepasar los 1588bytes.

Campo:	**Longitud:**	**Significado:**
Checksum	2 bytes	Siempre tiene FFFFh y no se usa.
Longitud	2 bytes	Número de bytes de cabecera + datos (máximo 1518).
HOPS	1 byte	Número de routers que ha atravesado el paquete. Inicialmente es 0 y cada router le suma 1. Si llega a 16 se destruye el paquete.
Packet type	1 byte	Indica qué tipo de paquete del protocolo NetWare que lleva este paquete IPX.
Dirección del nodo de destino	6 bytes	Normalmente el número de la tarjeta de red destino.
Dirección de la red de destino	4 bytes	Número IPX de la red de destino.
Socket de destino	2 bytes	Número del proceso (socket) al que va destinada la información.
Dirección del nodo de origen	6 bytes	Normalmente el número de la tarjeta de red de origen.
Dirección de la red de origen	4 bytes	Número IPX de la red de origen.
Socket de destino	2 bytes	Número del proceso (socket) que envía la información
Datos IPX	Hasta 1518	Información que transporta el paquete.

Figura 9: Distribuciónde la cabecera de un paquete IPX

Fuente: (García, 2013)

La identificación de los nodos dentro de la red se realiza a través de números asignados por el administrador de red mediante los direccionamientos entre redes, nodos y sockets de origen y destino, tomando en cuenta de igual manera las tarjetas disponen de números únicos (dirección MAC) localizando de esta manera grupos de trabajo, nodos en las redes y multiplexación, al instalar un servidor o router NetWare se agina una dirección IPX interna para que se puedan identificar dentro de la red y para cada tarjeta que disponga el servidor o router una dirección IPX externa o de red todo a través del protocolo IPX-RIP donde el tráfico sea direccionado entre redes.

Los números de identificación son arbitrarios y únicos, sin embargo, a diferencia de TCP/IP que funciona a través de secciones y subsecciones los IPX son completos y no tienen significado.

El problema que presenta IPX como gran desventaja es que puede funcionar en una LAN sin problema, pero en una MAN o WAN no puede ser enrutada ya que no puede controlar los broadcast, en las redes actuales se pueden utilizar múltiples protocolos de red, casi todos los sitios que disponen IPX también lo utilizan para el enrutado sobre el internet lo que ha provocado su desuso. (novell.com, 2001)

2.2.2.10 DECnet

Es una suite de protocolos peer-to-peer estandarizados creados por Digital el cual incluso hizo que Ethernet sea comercialmente aceptada, ya que este se basó en tecnología DECnet. Este conjunto de protocolos fue diseñado con la idea de conectar dos PDP-11

(minicomputadoras) como una arquitectura de red, originalmente contruido a base de tres capas para luego convertirse en siete capas compatible con el modelo OSI.

DECnet fue integrada en su sistema operativo VMS, luego integro hacia Ultrix, Apple Macintosh e IBM PC, variantes de DOS y Microsoft Windows con el nombre de DEC Pathworks, de esta manera permitía que los sistemas se conecten hacia las redes VAX como nodos terminales, posteriormente fue desarrollado para LINUX, sus diseños fueron desarrollados desde la fase I hasta la fase V +.

- Fase I: Apoyo a dos PDP-11 que se ejecutan con el sistema operativo RSX-11, la relación entre los nodos punto a punto.
- Fase II: Con soporte para redes de hasta 32 nodos con múltiples implementaciones que inter-operan entre sí, las comunicaciones entre procesadores punto a punto están limitadas solo a enlaces, las interfaces entre las tareas de programación y funciones de gestión de red son implementadas, además se implementa la carga de línea descendente y la transferencia de archivos mediante Listener (FAL)
- Fase III: Se implementa el soporte hasta 255 nodos punto a punto y enlaces multi-drop, capacidad para enrutar, puertas de accesos a otras redes incluidas como SNA, CCITT, X.25 entre otras.
- Fase IV y IV+: Se implementan siete capas: física, enlace, transporte, sesión, administración de redes y solicitud. Se apoya a las redes de hasta 64.449 nodos (63 áreas de 1023 nodos), enrutamiento jerárquico (áreas, nivel 1 y nivel 2 routers), conexión remota, soporte para DOS de 16 y 32 bits, plataformas Windows y Linux.

- Fase V y V+: Se soporta redes muy grandes con arquitecturas teóricamente ilimitadas, nuevos modelos de gestión de red, el paso de una red propia a una OSI, proporciona la conectividad de múltiples proveedores y compatibilidad con la arquitectura de red digital (ADN), estas características complementaron una arquitectura híbrida (ADN-OSI), todos los protocolos DECnet fueron diseñados por Digital Equipment Corporation (DEC) pero después se convirtieron en estándares abiertos. (Robbins, 2013)

2.2.2.11 X.25

Este conjunto de protocolos define la comunicación (formato y significado) entre equipos terminales de datos (ETD) y equipos de terminación del circuito de datos para terminales (DCE) que trabajan sobre redes de datos públicas todo orientado a la conexión a base de conmutación de paquetes, lo que quiere decir que: no se pierde la información, no se duplica ni se desordena, funciona a base de tres capas X.25 orientado a OSI Figura 10:

- Capa 1: define interfaces físicas entre el DTE y DCE referenciando y no definiendo a los estándares X.21 y X.21 bis, tomando en cuenta que debe elegir un número de circuito virtual el cual no puede ser duplicado.
- Capa 2: Asegura la comunicación lógica entre capas confiable entre el DTE y DCE utilizando los protocolos LAP y LAPB del grupo de protocolos HDLC.
- Capa 3: Administra las conexiones entre pares DTE ya sean a través de llamadas virtuales o circuitos virtuales permanentes.

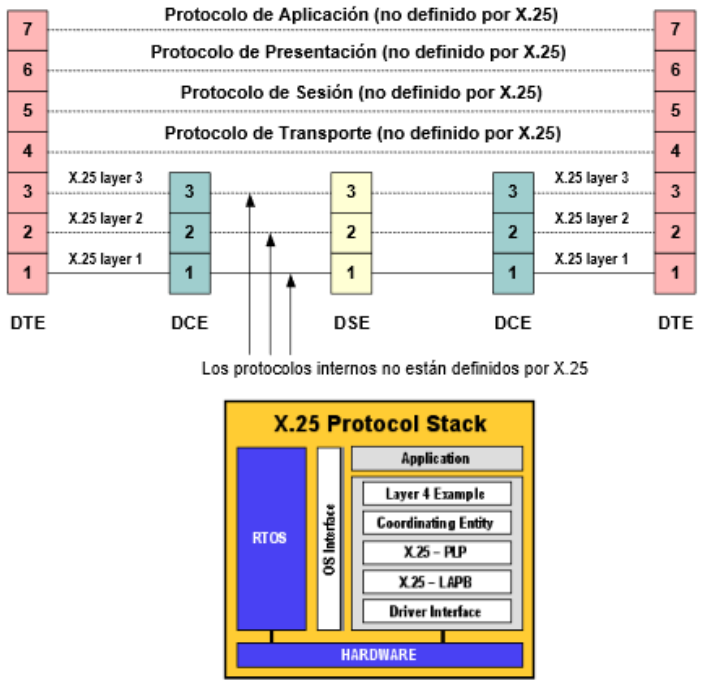


Figura 10: Estructura de capas del protocolo X.25

Fuente:(Torres, 2005)

X.25 permite la comunicación multiplexada hasta 4095 enlaces full dúplex simultáneos entre ETD-ETD y ECD-ETD, además permite realizar el control de errores utilizando el protocolo ARQ de ventanas deslizantes similar a los utilizados en HDLC. (Mayan & Alba, 2005, 2010)

2.2.2.12 TCP/IP

Es una suite de protocolos orientados a la conexión, siendo el estándar más utilizado por las redes a nivel mundial, se caracteriza específicamente por ser abierto y el cual es soportado por la mayoría de sistemas en red Figura 11, su funcionamiento lo hace prácticamente sobre

cualquier medio, por ejemplo, Ethernet, ADSL o fibra óptica, su direccionamiento lo hace asignando una dirección única a cada equipo conectado a la red así sea una muy extensa como el internet. Cualquier referencia acerca de este estándar por el hecho de ser abierto se lo puede encontrar en los RFCs (Request for Comments) detallando más a fondo las características físicas y lógicas de este grupo de protocolos.

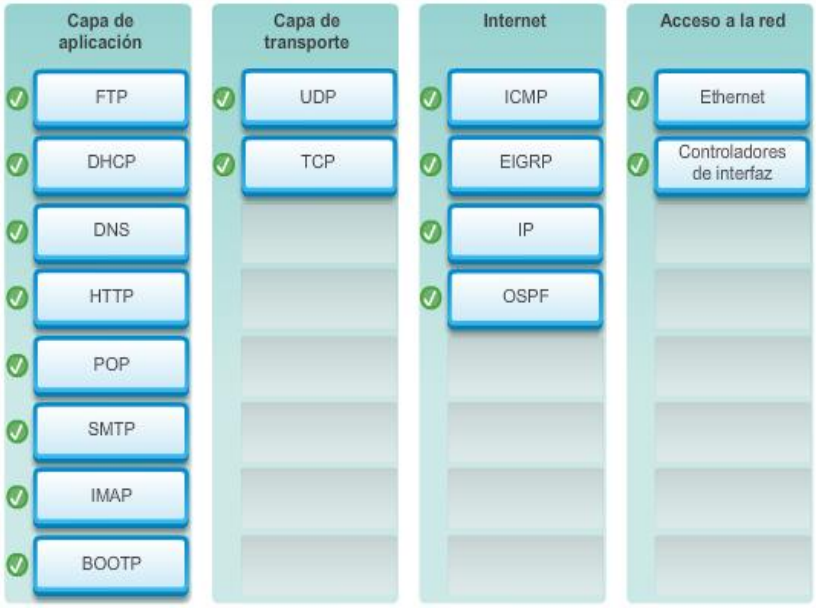


Figura 11: Suite de protocolos de la arquitectura TCP/IP

Fuente: (Rojas, 2014)

2.2.2.12.1 Arquitectura

TCP/IP cuenta con cuatro capas en las que incluye algunas del modelo OSI Figura 12, ya que fue creado primero.

A partir de que la capa de aplicación entrega el paquete de datos a la capa de transporte, esta recorre la pila de protocolos añadiendo o quitando por cada capa información de control al paquete para garantizar la transmisión a su equipo objetivo.

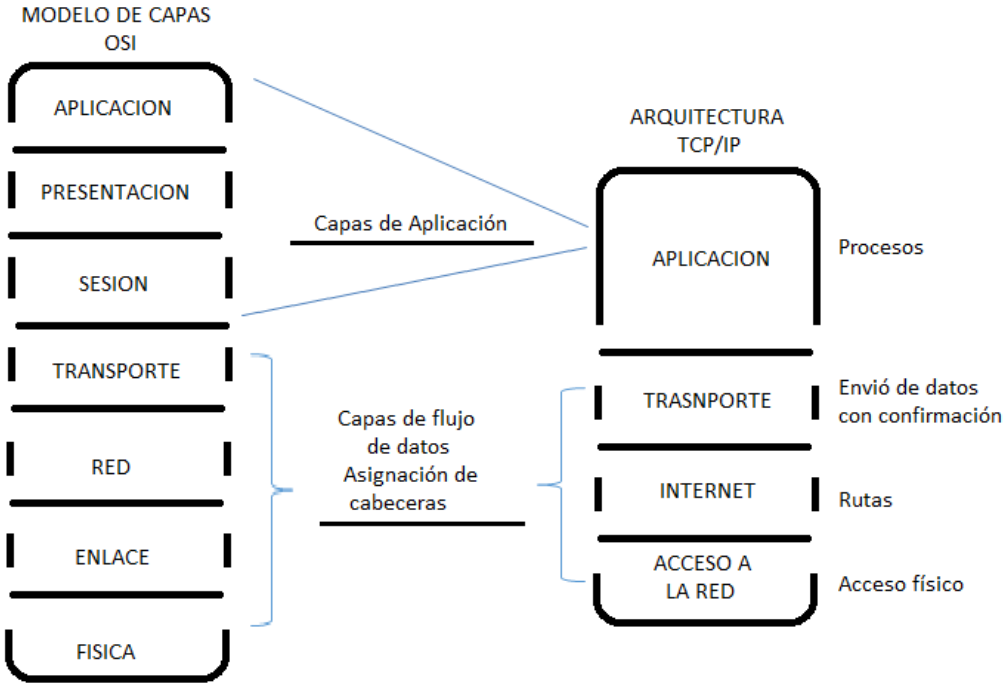


Figura 12: Comparación de capas entre el modelo OSI y TCP/IP.

Fuente: Elaborado por autor

Cada una de las capas de TCP/IP cumple una función específica que se detalla a continuación:

- Aplicación: define el software a utilizarse en la red y servicios que el usuario puede utilizar.
- Transporte: protege a los paquetes con el fin de que lleguen a su destino, ordenados y sin errores, regulando el flujo de la información.

- Internet: permite la transferencia de paquetes de recepción y emisión, controlando la comunicación entre los equipos.
- Acceso a la red: proporciona características del hardware que va a utilizar la red y conexión con los medios de transmisión.

La información que asigna a los datos por cada capa siempre van primero por lo cual se la denomina cabecera (head) y a este proceso encapsulado Figura 13, el equipo que envía la información la encapsula desde la capa de Aplicación hasta la capa de Acceso a la Red, pero si un equipo recibe la información realiza el proceso de forma contraria, eliminando cada una de las cabeceras al ir recibiendo desde la capa de Acceso a la Red tomando en cuenta que maneja una estructura de datos independiente mejorando a cada momento con la intención de que sean compatibles entre sí, buscando una eficiencia a nivel de todo el estándar.

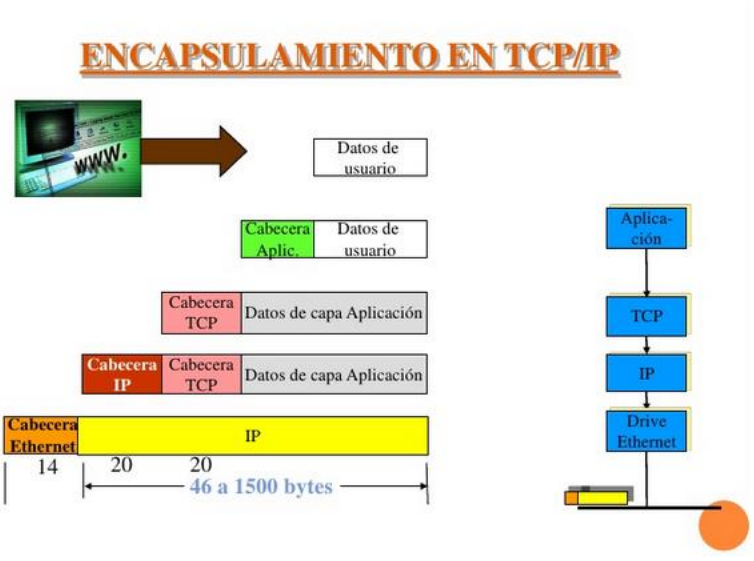


Figura 13: Empaquetado de datos por capas

Fuente: (García N. , 2012)

Para entender la suite de protocolos de TCP/IP se debe tomar en cuenta que la arquitectura de dichos protocolos ve a todas las redes como iguales para la conexión, sin importar si es una LAN o WAN, la conexión de estos debe disponer de compuertas para comunicarse entre redes a esto se le denomina enrutamiento, en este caso los routers (compuertas) que permiten localizar un camino para la transmisión, para dicha comunicación las redes deben disponer identificadores físicos y lógicos en la capa de red y la capa de acceso respectivamente a estos identificadores se les denomina dirección Física (MAC) y dirección lógica (IP) identificando a la red que pertenece un computador y a ella misma, y en el caso de duplicación de direcciones IP se utiliza subredes para diferenciarlas.

Hay que tomar en cuenta que los protocolos TCP/IP están orientados a transmitir paquetes independientemente de la arquitectura de una red, sin embargo en el caso de Ethernet se comunica solo conociendo la dirección física del equipo, así cada equipo que cuente con una dirección IP debe disponer de un mecanismo para traducirla a una dirección física logrando la comunicación, esta traducción se la realiza por medio del protocolo ARP, en cada solicitud de dirección IP destino, el equipo que contesta actualiza su tabla temporal de conversiones para posteriores transmisiones, siendo la interfaz la que compara su tabla con la IP solicitada, sí existe coincidencias se adjunta al paquete y se envía, sin embargo hay que tener en cuenta que sí un equipo falla la dirección física cambia a lo cual los paquetes que se envían hacia este se perderán constantemente ante esto hay que eliminar periódicamente las direcciones.

También dentro de la suite ya mencionada existe el protocolo IP el cual forma parte de la capa de internet, este realiza la distribución de los paquetes pero no orientado a la conexión, los cuales pueden viajar por diferentes caminos para llegar al destino requerido sin garantizar que la entrega haya tenido éxito a esta unidad de conexión se la denomina datagrama, si el datagrama a transmitir es demasiado grande lo puede fragmentar con un tamaño máximo de 1500 bytes denominándole MTU, una vez que la transmisión de ha logrado el datagrama es reensamblado, utiliza direcciones lógicas IP de 32 bits, si el paquete enviado no llega a su destino puede ser eliminado por medio del protocolo ICMP. (Naranjo, unavarra.es, 2013)

2.2.2.13 AppleTalk

Protocolo creado a principios de los 80's por Apple Inc., con la intención de compartir recursos como archivos en impresoras identificados como nodos en forma jerárquica entre diferentes usuarios de Macintosh, siendo implementaciones de red para el primer sistema distribuido cliente/servidor.

Su interfaz es de características transparentes y su desarrollo fue creado y mejorado mediante 2 fases: La fase 1 trabaja solamente a nivel local (redes no extendidas) con máximo 135 clientes y servidores, la fase 2 es creada con la principal idea de mejorar las redes locales a redes extendidas pudiendo realizar el trabajo en las dos, con 235 clientes como servidores.

De igual forma que OSI, contiene sus capas y protocolos Figura 14, Appletalk las contiene con su respectiva equivalencia en la capa física y enlace de datos, manteniendo de

igual que en TCP/IP dependencia de acceso a medios en las capas bajas como Ethernet, Token Ring y FDDI, de estas las implementaciones que dispones son:

- EtherTalk (IEEE 802.3)
- LocalTalk (Interfaz de red)
- TokenTalk (IEEE 802.5/Token Ring)
- FDDITalk (FDDI)

Mediante estas implementaciones la capa de enlace de datos realiza traducciones de direcciones para la comunicación de sus interfaces.

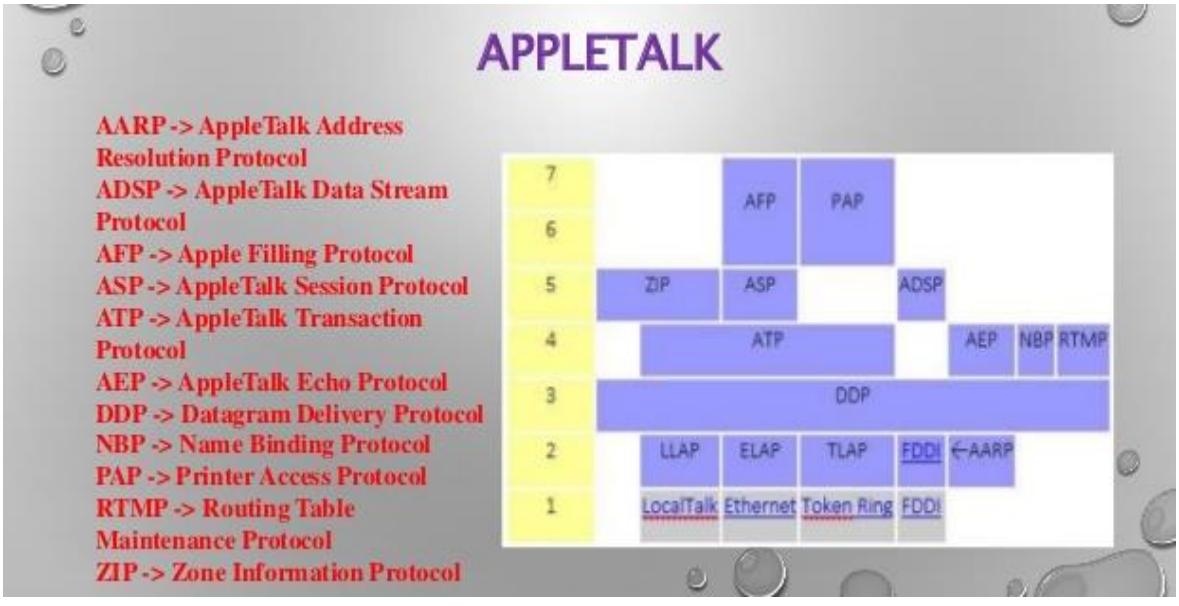


Figura 14: Correspondencia de los protocolos AppeTalk y modelo OSI

Fuente: (Castillo, 2015)

Este protocolo tiene componentes básicos como:

- Sockets: punto donde se comunican las capas superiores y la de red de protocolo al entregar el datagrama, pudiendo ser asignado los sockets estática o dinámicamente.
- Nodos: Cualquier dispositivo que esté conectado a la red, tomando en cuenta que los procesos realizados dentro de estos son sockets.
- Redes: La conexión entre varios nodos y uno o varios cable lógico y físicos.
- Zonas: Un grupo de nodos dentro de la red configurados por el administrador que pertenecen a una misma zona. (cisco, 2007)

2.2.2.14 NetBEUI.

Este protocolo es una implementación sobre NETBIOS (Network Basic Inpup/Ouput System) al cual se le denomino NetBEUI (NETBIOS Extended User Interface), tomando en cuenta que parte de hacer la distribución de aplicaciones por un Main Frame lo que causa un descontrol en la administración del sistema y provoca demasiado uso de la LAN, que posteriormente a la unión entre IBM y Microsoft se integró a la plataforma Windows 3.x, 95 y 98, que poco a poco fue perdiendo terreno en las distribuciones posteriores en las cuales apenas se mencionaba ya que por algunos análisis se descubrió que este protocolo abusaba de los mensajes broadcast.

El rendimiento en redes o segmentos locales es muy alto por su pequeña cabecera, sin embargo su rendimiento en redes WAN es deficiente. Desde su aparición y mejora de sus versiones por ejemplo NetBEUI 3.0 interactúa con interfaz de controlador de transporte TDI

sin ser en este caso una completa mejora de NETBIOS, pero en Windows NT es compatible e interoperable con NETBEUI y versiones anteriores de Microsoft.

A pesar de ser el protocolo más rápido proporcionado por Windows NT, puede hacer enrutamiento en Token Ring y operar en las capas 3 y 4 del modelo OSI no es routeable ya que funciona en redes LAN sin problema pero en WAN su rendimiento es muy pobre debido a que carece de una capa de red siendo de esta manera no encaminable a lo cual es necesario el uso de puentes para comunicación entre redes.

Como características principales se puede decir que utiliza el protocolo SMB (System Message Block) permitiendo compartir discos, archivos, impresoras y compuertas COM siempre y cuando lo haga con su igual correspondiente en caso de servidor o cliente, posteriormente a esto NETBIOS con NetBEUI forman un nuevo entorno con características mejoradas como: redirigiendo peticiones de red a los servidores adecuados en la capa de aplicación provocando que una computadora cliente distinga todos los recursos de red como si fueran locales, la comunicación de nodos par a par proporcionados por un lenguaje y los formatos correspondientes en el nivel de aplicación, en la capa de sesión NETBIOS administra las comunicaciones establecidas, en la capa de transporte NetBEUI proporciona nos servicios necesarios para trasladar los datos pudiendo estar conectado al acceso telefónico y a la vez a TCP/IP, para definir la interfaz de red utiliza NDIS (programa de interfaz de control para admitir varios protocolos de red un una sola NIC) para el control de enlace lógico y el controlador NIC para el control de acceso al medio.

Tomando en cuenta lo descrito NETBIOS podrá ser trasportado ya sea por TCP/IP para salir de una red o NetBEUI para comunicación local tomando en cuenta que este último necesita de NETBIOS para acceder a la capa de sesión. (Cruz, 2011)

2.3 Protocolos seguros

Disponer de seguridad en una red no significa solo tener un antivirus o un firewall, más bien es realizar un análisis que permita identificar en que capas de la estructura de la red o modelo utilizado, se pueda establecer seguridad en todo momento Figura 15.

La mayoría de entidades que crean una red con el objetivo de transmitir datos asumen que al colocar un software antivirus, en el mejor de los casos un firewall y una persona que administre la red ya tienen asegurada su información, pero este error puede costar mucho dinero puesto que la información sin el respectivo y adecuado monitoreo es muy vulnerable. Diversas empresas orientadas a desarrollar mecanismos para identificar el lugar más idóneo para controlar el flujo de la información han creado aplicaciones que con su respectivo estudio, de acuerdo a sus necesidades y basándose en el modelo OSI o TCP/IP, la meta es no permitir información alterada, muchas veces se piensa que dicha información es peligrosa cuando proviene del exterior de una red, sin embargo la mayoría de ataques suelen darse desde el interior de la misma.

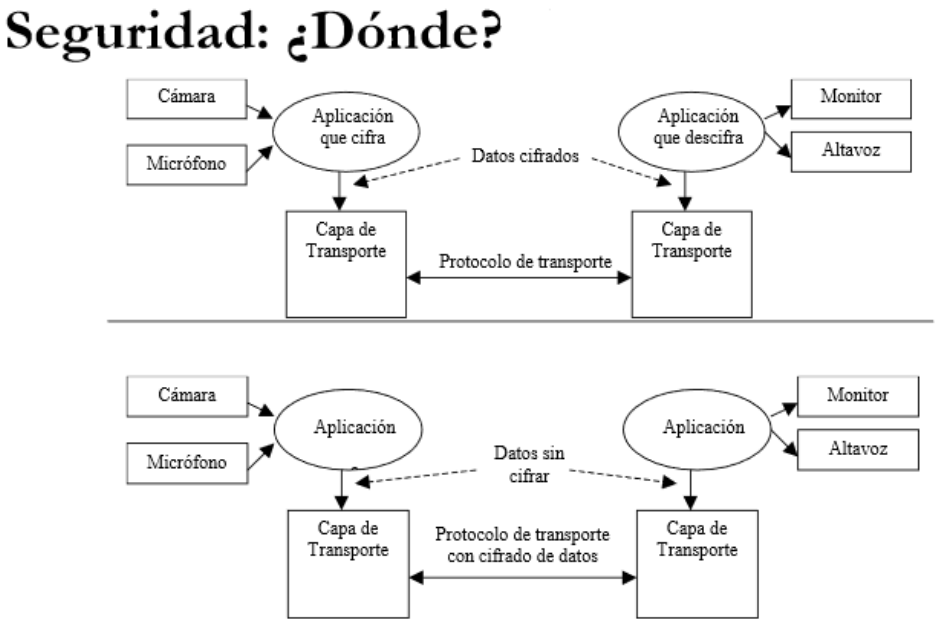


Figura 15: Descripción de puntos de seguridad a ser analizados

Fuente: (Enguita, 2009)

Controlar datos que han sido ya identificados y documentados por uno o varios antivirus no garantiza en ningún momento que la red esté libre de ataques puesto que un usuario dentro puede estar ingresando de forma normal con lo cual no se puede identificar fácilmente daños a la información.

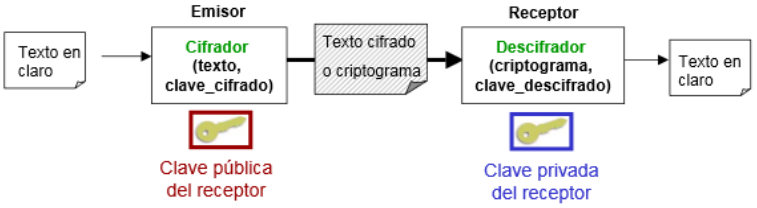
2.3.1. Protocolo de seguridad

Tomando en cuenta que un protocolo es un conjunto de reglas para establecer la comunicación se adiciona la palabra seguridad, indicando de esta manera, que al utilizar este tipo de protocolos se pretende que un sistema pueda soportar y defenderse de posibles ataques mientras transmite información por un canal seguro de datos, siguiendo parámetros respecto a riesgos a los cuales está expuesto, en muchos casos se utilizan protocolos dentro

de los dispositivos que permiten segmentar la red y la comunicación está controlada en forma individual VLANs en switches o utilizando reglas con las cuales se permite transmitir determinados datos y de nodos permitidos ACLs pero, muchos ataques son realizados con conocimiento de estas técnicas saltándoselas.

Aduciendo que un protocolo puede controlar un ataque este debe disponer de características (seguridad criptográfica) que le permitan controlar cierto nivel de riesgo a la que la información está expuesta, los protocolos de seguridad en su mayoría dependen de claves encriptadas al azar y utilizando claves largas, con algoritmos de criptosistemas mas el texto a transmitir, sean estos algoritmos simétricos que no son muy seguros por ser privados y no estar expuestos a muchos ataques o asimétricos que su nivel de seguridad es más alto por ser públicos y tener que disponer de criptografía robusta para permitir la salida de la información fuera de la red Figura 16, sin embargo hay que tener en cuenta que en la actualidad ya no solo el texto transmitido es atacado, a esto se adiciona que los ataques se los realiza a las claves, a las encriptaciones y a los protocolos de seguridad, de ahí el por qué un sistema debe defenderse y el porqué de los protocolos de seguridad a estudiarse sea estos con cifrado de enlace (capa 2) en los cuales cifra todo el mensaje incluyendo cabeceras sugiriéndose que los nodos intermedios que reciben la información deben tener la capacidad de descifrar o cifra nuevamente para procesos de encaminamiento o cifrado extremo a extremo (capa 7) las cabeceras no se cifran desde los nodos origen hasta el final, solamente el contenido del mensaje.

- Cifrado/Descifrado asimétrico con clave pública:



- Firma digital y autenticación:

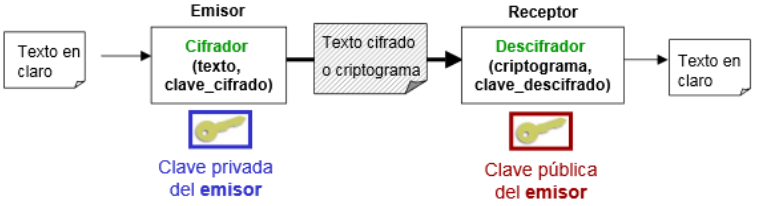


Figura 16: Estructura de claves simétricas y asimétricas

Fuente: (Romero M. , 2006)

El fin de utilizar los protocolos de seguridad es:

- Manejo y almacenamiento de claves (utilizando algoritmos de seguridad)
- Privacidad en la información transmitida procurando que siempre sea confidencial
- Muchos sistemas ingresan sea o no manipulados por un tercero hacia la información requerida, sin embargo al verificar que dicho sistema utilizo la información puede negar su uso, para esto se utiliza certificados digitales, los cuales permiten indicar quien estuvo presente durante la visita sin poder negar su presencia a esto se le conoce como no repudio**.**
- Permite autentificar que el usuario de la información es el real, el autorizado por los administradores y no un posible ataque.

2.3.2 Ataques más frecuentes a la red

- Contraseñas nulas o por defecto: Son contraseñas que dispone el hardware y que son propias del fabricante, permiten realizar las configuraciones iniciales, sin embargo muchos administradores se olvidan de cambiarlas, es el camino de inicio para un ataque.
- Contraseñas compartidas por defecto: Son claves generadas para desarrollo o pruebas, sin embargo al olvidarse de modificar estas claves y poner el sistema en ejecución cualquier usuario con una clave por defecto igual puede ingresar.
- IP spoofing: Instalación de una maquina remota en la red, identificando vulnerabilidades y aprovechándose de los recursos de esta, muchas veces los atacantes asistidos por herramientas disponibles en la web.
- Eavesdrooping: Se tratan de sistemas comprometidos de los cuales dan paso a un atacante, este reúne información de nodos que intercambian información en la red, rastreando la conexión entre estos.
- Vulnerabilidades de servicios: Al ser desarrollados los sistemas muchas veces no se toma en cuenta que pueden quedar errores y cuando existe un ataque estos son aprovechados para comprometer sistemas completos.
- Vulnerabilidades de aplicaciones: Las fallas que un atacante identifica en aplicaciones de escritorio y estaciones que manejen correos normalmente suelen ser aprovechadas para implantar código malicioso como virus caballos de Troya para comprometer en el momento o a futuro un sistema más aún si este dispone de

privilegios de administrador, en muchos casos los clientes de correo al no saber reconocer estos ataques ayudan a que el proceso de comprometimiento del sistema sea más efectivo.

- Ataques de denegación de servicio (DoS o DDoS): Este tipo de ataques suele ser el más común, ya que se ataca a los recursos de la red o a un servidor para que estos no puedan responder rápidamente a los usuarios y mientras tanto el atacante puede manipular o coordinar conjuntamente con otros atacantes el saqueo de la información disponible, esto se lo puede realizar desde otro servidor o muchas veces desde los mismos dispositivos que están disponibles en la red provocando un autoataque.
- Rastreadores o sniffers: Siendo software especializado para interceptar tráfico que es transportado por su camino sea físico o inalámbrico, este software pone a sus interfaces de recepción en modo promiscuo, lo que permite que reciba todo tipo de datos para ir analizándolos uno a uno procurando obtener toda la información posible entre las entidades que se están comunicando.
- Ataques de hombre en el medio (o man-in-the-middle attacks): Entre una comunicación de dos entidades se implanta una tercera ya sea en forma física o lógica, la cual recepta información de los nodos y les responde a cada uno como si se estuvieran comunicándose entres si, proporcionando datos importantes de los cuales el atacante se sirve.

2.3.3 Protocolos de autenticación y establecimiento de claves de sesión

Para establecer comunicación no basta solo con la autenticación de nodo a nodo, es también necesario que puedan establecer mecanismos de encriptación que a la ves estos se puedan comunicar entre cada nodo que recibe la información, el objetivo de esto es no permitir que un atacante al interceptar el tráfico pueda descifrarlo, todo mediante el uso de los protocolos de establecimiento de claves y los protocolos criptográficos seguros.

Al acceder a cualquier red en la actualidad la mayoría de estas solicitan un usuario y clave para poder confirmar su identidad, esto se logra gracias a algunos protocolos que permiten realizar este proceso denominado autenticación y los que permiten establecer claves durante la sesión, sin embargo hay que tomar en cuenta que los mecanismos de autenticación deben ser muy robustos ya que los protocolos son más vulnerables que los algoritmos de cifrado, los más utilizados son:

2.3.3.1 Protocolos de la capa de aplicación

- Kerberos: Es el protocolo de autenticación más utilizado, identifica a los usuarios a través de una gran biblioteca de claves con encriptación que son utilizadas dentro del protocolo para tener acceso a un dominio, la clave que utiliza el usuario es comparada con las claves almacenadas y si es correcta autentica al usuario, este puede que solicite tener acceso a otros servicios a lo cual es necesario en muchos casos otra clave de autenticación, los servicios interactúan directamente con Kerberos y no con el usuario creyendo este, que está comunicándose directamente con el protocolo y en

muchos casos los atacantes intentan tener acceso a servicios no permitidos sin darse cuenta que solo han atravesado la primera etapa con la clave y pueden ser identificados con facilidad por un protocolo de seguridad adicional.

- SSH (Secure SHell): este protocolo permite crear conexiones seguras sobre redes no seguras, la mejor opción en lugar de utilizar programas de acceso no seguro como telnet, ftp, rlogin, entre otros.

  Se trabaja con un terminal cifrado con criptografía de clave pública utilizando diversos mecanismos de autenticación, tunneling de conexiones TCP para proteger protocolos inseguros atravesando con facilidad los cortafuegos, soporta métodos de conexión externa como es el caso de Kerberos, después de haber iniciado la conexión el cliente tiene la posibilidad de verificar si continua conectado al mismo servidor en las siguientes conexiones, interfaz gráfica segura a través de X11, en caso de reenvío de puerto por parte del servidor se pueden cifrar protocolos inseguros para garantizar la comunicación segura.

- Radius: Este protocolo permite la primera conexión a la red, para posteriormente redirigirla a un servidor con software Radius que contiene los datos de autenticación en formato encriptado el cual puede aceptar o rechazar la conexión, y el usuario tiene que autenticarse ante este para poder continuar con la conexión al resto de la red si es rechazado simplemente lo intenta otra vez, si se necesita autenticación para servicios adicionales esta es manejada a través de otros protocolos.

- TACACS+: Este protocolo es una mejora de Radius luego de la experiencia que tuvo Cisco, al cual lo mejoro con encriptación no solo de la clave sino también el nombre del usuario y datos asociados con mecanismos más robustos, es escalable y puede proveer de servicios adicionales de autenticación para varias capas lo que le permite relacionarse con Kerberos.

Este tipo de protocolos son muy efectivos con usuarios básicos, sin embargo si un atacante tiene acceso a las bibliotecas de las claves se termina la seguridad o en el caso de que este tenga acceso físico con un simple punto de acceso conectado antes del protocolo de autenticación simulando un ataque Man in the Middle la seguridad se ve muy comprometida, por experiencia, se puede realizar un cambio de IP en forma constante durante tiempos cortos con lo que los protocolos de autenticación no reaccionan con rapidez.

2.3.3.2 Protocolos de la capa de Transporte

- SSL (Secure Socket Layer): Este protocolo es de uso público para utilización de canales seguros sobre TCP, con el fin de realizar conexiones seguras a los servidores sin importar el sistema operativo que este al extremo de un canal.

Compuesto por dos capas que le permite encriptar los datos al ser transportados:

✓ SSLRP(SSL Record Protocol): Construye un canal de comunicaciones seguro sobre el cual encapsula los protocolos de nivel alto.

- ✓ La segunda capa está a la vez compuesta de tres protocolos que se encargan de gestionar la negociación de los algoritmos de cifrado, señalizar problemas en la sesión establecida y a través de un byte notificar cambios de estrategias de cifrado.

- ✓ *Funcionamiento de SSL*

El protocolo SSL a través de cliente hace una conexión informando acerca de los sistemas criptográficos que dispone al servidor y este responde con un identificador indicando su clave y los sistemas criptográficos que soporta, el cliente elige el sistema criptográfico, verifica la clave pública del servidor y se genera una clave cifrada con la del servidor, si algún atacante quisiera descifrar la información no la lograría porque en este punto solo se fragmenta la conexión y si quisiera conectarse hacia cualquiera de las dos entidades tendría que generar otra clave diferente, para esto autenticarse entre el cliente y servidor nuevamente, determinando de esta manera durante todo el proceso que los mensajes transmitidos no han sido modificados, que ninguna persona sin autorización puede leer su contenido transmitido y solo recibe el destinatario correcto.

A través del protocolo SSL Handshake se genera parámetros criptográficos funcionando sobre SSL Layer Protocol, y su negociación es en primera conexión y posteriores, al utilizar los protocolos de capas superiores SSL utiliza la versión 3.0 la cual trabaja en forma transparente con los protocolos de TCP asignados números de puerto por el IANA Figura 17, estos también son utilizados en TLS, los servicios de seguridad de SSL son confidencialidad a través del cifrado y descifrado, autenticación a través de autenticación de certificado y criptosistemas de clave pública, integridad con el código MAC (Message

Authentication Code), y no repudio a través de certificado y firma digital. De igual manera sus desventajas al utilizarse son: Solo trabaja con TCP, nada de UDP o IPX lo cual si se intenta provocaría un cifrado y descifrado por separado para cada paquete UDP con claves distintas, no repudio solo lo implementa si ambos extremos tienen certificados en caso contrario desaparece este proceso, ineficiencia debido al handshake inicial solo cachea sesiones para HTTP y necesita hardware especializado para acelerar el tráfico SSL tarjetas, dispositivos externos y balanceadores de carga para SSL, esto provoca un costo adicional por extremo.

Identificador de protocolo	Puerto TCP	Descripción
https	443	HTTP sobre SSL
smtps	465	SMTP sobre SSL
nttps	563	NTTP sobre SSL
ladps	646	LDAP sobre SSL
telnets	992	TELNET sobre SSL
imaps	993	IMAP sobre SSL
ircs	994	IRC sobre SSL
pop3s	995	POP3 sobre SSL
ftps-data	989	FTP-Datos sobre SSL
ftps-control	990	FTP-Control sobre SSL

Figura 17: Números de puertos TCP sobre SSL

Fuente: (Romero M. d., 2006)

- TLS: Este protocolo es una evolución de SSL, manteniendo el establecimiento de conexión segura entre el cliente y servidor procurando un entorno seguro sin ataques, sin embargo en este caso solo el servidor se autentica, garantizando su identidad pero el cliente no lo hace ya que es necesario una infraestructura de claves PKI para los

clientes provocando costos muy altos, con este protocolo se evita el eavesdropping y se mantiene la integridad del mensaje en la comunicación.

La transmisión la realiza por fases: negociación para utilizar algoritmos criptográficos para autenticarse y cifrar información pudiendo usar criptografía de clave pública RSA, Diffie-Hellman, DSA, cifrado simétrico con RC2, RC4, IDEA, entre otros, funciones hash con MD5 o SHA, la autenticación y claves mediante certificados digitales y por último la transmisión segura que es cifrada y autenticada.

El fin de este protocolo es mantener una seguridad criptográfica, las aplicaciones con diferentes características deben poder intercambiar criptografía sin importar el conocimiento de los códigos entre los terminales, este protocolo permite incorporar nuevos algoritmos de criptografía, tiene esquema de cache de sesiones reduciendo de esta manera la conexión desde cero, evitando costos muy altos que tienen los algoritmos.

El funcionamiento de este protocolo está dividido en dos niveles:

- ✓ Protocolo de registro TLS: protocolo de bajo nivel implementado sobre TCP trabajando con conexión privada utilizando protocolos de cifrado simétrico el cual también puede ser utilizado sin encriptación, y con conexión fiable verificándose la integridad en el transporte.
- ✓ Protocolo de mutuo acuerdo: En este la identidad del interlocutor puede ser autenticada utilizando clave pública, la negociación de un secreto compartido segura, la negociación es fiable evitando que la negociación sea modificada sin ser detectado por los interlocutores. (Navarro, Ubilla, & Tejeda, 2014)

2.3.3.3 Protocolos de la capa de Red

- IPSec: Este protocolo de seguridad es el más importante a describirse ya que proporciona de mejores servicios de seguridad a nivel de la capa 3 y a todos los protocolos de capas superiores basados en IP, a diferencia de los ya descritos que para autenticar, establecer o cifrar claves necesitan modificar el código de las aplicaciones, de lo cual IPSec no hace uso.

Es un conjunto de protocolos criptográficos que permite asegurar el flujo de paquetes, permite la autenticación mutua, y establece parámetros de seguridad criptográficos todo esto para el protocolo IP, integrándose hacia la versión IPv4 e IPv6, está apoyado por la IETF y la mayoría de los equipos de comunicaciones lo tienen incorporado, además trabaja a base de un sistema abierto lo que garantiza a los usuarios seguridad y actualización en los sistemas operativos más comunes e implementa tecnología PKI, implementación de sistemas más robustos e interoperabilidad entre fabricantes.

Su diseño está orientado a proporcionar seguridad de alta calidad basada en criptografía que ofrece un conjunto de servicios como es el control de acceso, integridad sin conexión, autenticación del origen de los datos, protección antireplay, confidencialidad (encriptación) y confidencialidad limitada del flujo de tráfico, todos estos servicios para el nivel descrito y los superiores, combinando tecnología de clave pública, algoritmos de cifrado, algoritmos hash y certificados digitales Figura 18, siendo este protocolo diseñado de forma modular de modo que se utiliza algoritmos seleccionándolos sin afectar otras partes de la implementación, de igual manera se aclara que dentro de este protocolo también existen

algoritmos estándar que soportan todas las implementaciones para asegurar la interoperabilidad como son: DES y 3DES para cifrado, así también MD5 y SHA1 para funciones hash.

Figura 18: Tecnologías que utiliza IPSec

Fuente: (Perez, 2001)

En la estructura de seguridad IP se encuentra conjuntos de algoritmos usados para autenticar y cifrar flujos en las direcciones, a estos conjuntos se les denomina asociaciones de seguridad, IPSec basa su protección en asociaciones de seguridad, en este caso para decidir la salida de un paquete lo realiza mediante el parámetro SPI que es un índice a la base de dados de asociación de seguridad SADB, junto con la dirección de destino de la cabecera de un paquete y entre estos dos deciden qué asociación de seguridad proporcionar para el paquete saliente, en el caso de ser multicast la salida se proporciona la seguridad a todo el grupo, duplicándose para todos los receptores de dicho grupo, de acuerdo a esto puede haber varias asociaciones de seguridad para un grupo utilizando direfentes SPIs con varios niveles de seguridad dentro del grupo.

Dentro de IPsec se derivan dos componentes de seguridad:

- AH (Authenticatión Header) y ESP (Encapsulating Security Payload), son protocolos de seguridad que protegen del tráfico IP.
- IKE (Internet Key Exchange) es un protocolo de gestión de claves, los cuales permiten a dos nodos negociar las claves y parámetros para establecer conexiones AH o ESP.

El protocolo AH esta designado por el IANA con el número decimal 51 por lo que ya no utiliza el valor 6 o 17 que son asignados para TCP o UDP respectivamente, este protocolo permite encapsular la cabecera basado en el algoritmo HMAC para su autenticación su funcionamiento descrito en Figura 19, es insertada entre la cabecera IP y los datos transportados, garantiza la integridad de la cabecera y autenticidad de los datos, sin embargo a los campos: TOS, TTL, flag y checksum no.

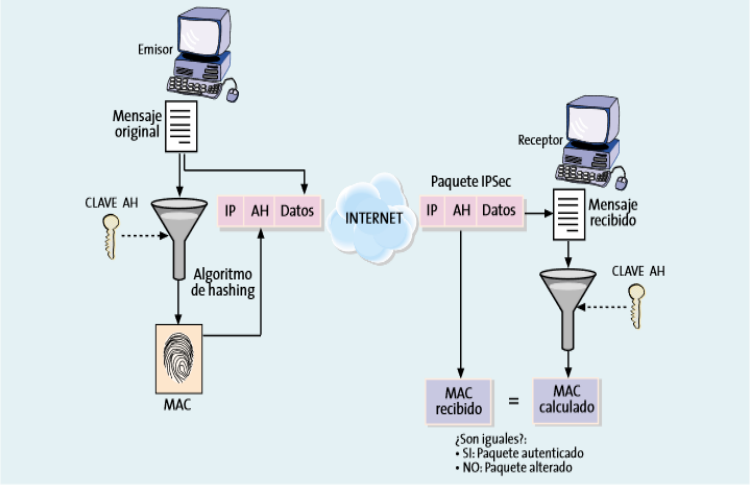


Figura 19: Estructura de funcionamiento del protocolo AH

Fuente: (Perez, 2001)

Se puede decir que la seguridad del protocolo AH se basa en el cálculo del MAC entre el emisor y receptor, de coincidir todo el mensaje está correcto, de no coincidir el mensaje fue alterado.

El protocolo ESP es designado con el número 50 por el IANA, proporciona confidencialidad de los datos especificando su modo de cifrado y como se incluye en un datagrama IP, de igual manera puede ofrecer servicios de integridad y autenticación de cabecera similar a AH pero ofrece más servicios por lo tanto su estructura es más compleja proporcionando cabecera y cola que rodean los datos a ser transportados siendo estos cualquier protocolo IP (TCP, UDP, ICMP o protocolos IP completos) a través de caracteres de relleno que aumenta la longitud real del bloque mediante el campo pad len y a través de algoritmos de cifrado de bloque, protege la información dentro de la cabecera por lo tanto si existe un ataque este no podría saber qué tipo de datos son transportados ya que se encuentran ocultos.

ESP puede proveer autenticación por medio de la HMAC de AH con la diferencia que esta solo autentica la cabecera ESP y la carga útil encriptada no todo el paquete IP, siendo muy útil ya que para un atacante sería posible ver que la cabecera es ESP pero no podría obtener información de la carga útil.

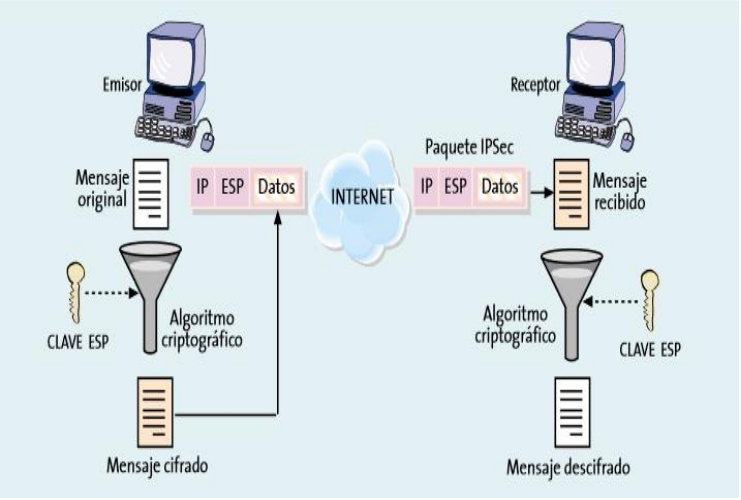


Figura 20: Estructura de funcionamiento del protocolo ESP

Fuente: (Perez, 2001)

Para que un ataque no tenga éxito debe existir un acuerdo entre el emisor y receptor de la distribución de las claves en forma segura tanto para el algoritmo de cifrado a utilizar como el hash y todo el resto de parámetros Figura 20.

IPSec transmite información de dos modos para ESP o AH:

- Modo de transporte: en el cual solo la carga útil es cifrada, el enrutamiento permanece tal como se designó al inicio por los protocolos, sin embargo cuando se utiliza la cabecera AH las IP no pueden ser traducidas porque las capas de transporte y aplicación están aseguradas por un hash y estas no pueden ser modificadas, en este modo se invalida dicho hash, en este caso el protocolo AH es modificado de forma ligera con un proceso de arrastre que sirve de conexión entre las cabeceras, en el caso de ESP de igual manera se encapsula solo la carga útil para la comunicación extremo a extremo quedando libres las cabeceras para su respectivo direccionamiento.

- Modo túnel: todo el paquete con sus cabeceras en cifrado y autenticado siendo nuevamente encapsulado en un nuevo paquete IP para su enrutamiento proporcionando una comunicación segura red a red en un canal inseguro, en este caso el protocolo AH y ESP es sellado dentro de un paquete IP con un identificador para prevenir posibles modificaciones durante el tránsito, al llegar a su destino son retiradas las cabeceras IP y AH quedando el datagrama original y enrutado normalmente, la diferencia en ESP radica en que el visitante o atacante no puede visualizar con lo cual es imposible desencriptar sin sus respectivas claves.

Protocolo de control IKE permite realizar la negociación de los algoritmos criptográficos a utilizarse en forma automática, en este caso el IKE es un protocolo de control, definido por el IANA con el número 9 para realizar la gestión de claves y las SAs correspondientes, es importante destacar que este protocolo no funciona solamente en IPSec sino que también puede ser utilizado en casos como OSPF o RIPv2.

IKE es un protocolo hibrido definido por otros que se refieren a la sintaxis de la comunicación y la forma de transferencia segura de claves entre dos partes que no se conocen, teniendo como objetivo principal establecer qué asociación de seguridad necesita utilizar, mediante una conexión cifrada y autenticada. Figura 21

Para establecer esta comunicación y crear nuevas claves IKE utiliza el algoritmo HMAC y las claves derivadas de la principal la consigue mediante el algoritmo Diffie-Hellman haciendo uso adicional del paso de autenticación del secreto compartido, siendo una cadena de caracteres conocida únicamente por los dos extremos que quieren establecer una

comunicación IPSec, como primera fase cada extremo utiliza la función hash sin revelar su valor, es seguro mientras no sean muchos secretos compartidos entre varios extremos, por otro lado en los estándares IPSec se encuentran previstos métodos de autenticación utilizando certificados digitales X509v3 con los cuales los nodos pueden probar su identidad mediante la estructura PKI.

Y como segunda fase un canal seguro creado por IKE es utilizado para crear los parámetros de seguridad asociados a un protocolo determinado en el caso de IPSec se negocian las características para AH o ESP, el nodo que inicia la conexión ofrece sus opciones de políticas de seguridad el receptor acepta y comienza la transferencia tomando en cuenta que ambos conocen el tráfico a transmitir de acuerdo a eso te utiliza los protocolos ESP o AH.

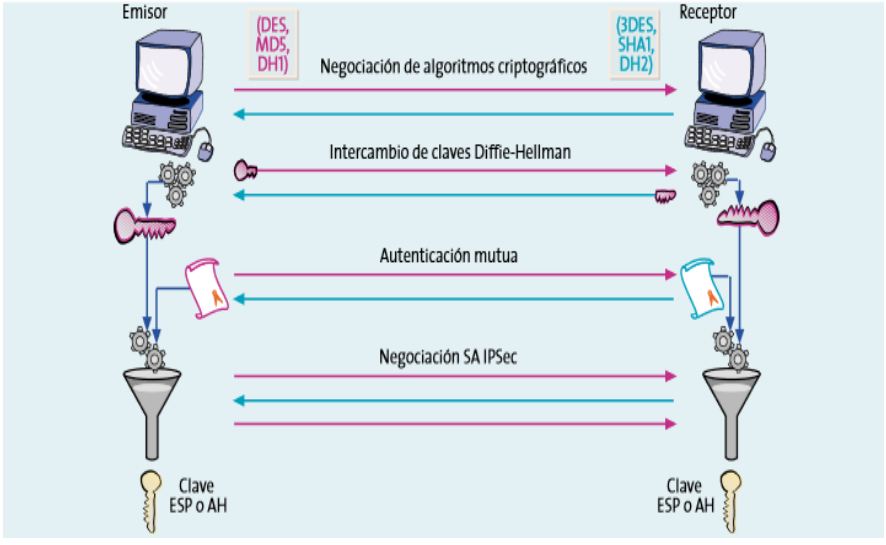


Figura 21: Estructura de funcionamiento del protocolo IKE

Fuente: (Perez, 2001)

Por último se concluye que IPSec es un protocolo que complementa a la carencia de seguridad en IP, es indispensable en las transacciones que son en su mayoría son críticas sobre todo en transacciones de empresas tomando en cuenta que la seguridad la proporciona sin importar la aplicación utilizada. (Surnoza & Figueira, 2013)

Con las características mencionadas se debe hacer uso de los protocolos criptográficos que permiten el transporte de datos seguros a nivel de aplicación a sabiendas que estos deben reunir las siguientes características:

- Establecimiento de claves
- Autenticación de usuario/servidor
- Cifrados simétricos y autenticación de cada mensaje
- Métodos de no repudio

Al gestionar claves se siguen políticas con parámetros en base a: la reutilización de claves, privilegios prolongados a usuarios, en especial a los que ya dejan de pertenecer al sector de administración o manejo de datos, usuarios que comparten claves con otros, estas políticas permitirán que las claves generadas para cada entidad o procesos no se vean comprometidas fácilmente por ataques.

Para gestión de claves, se utilizará jerarquías de las mismas, que teniendo un nivel superior pueden cifrar a las de nivel inferior, esto quiere decir que se debe crear claves para generación de otras claves de sesión, claves para transporte de claves de sesión, claves de cifrado de claves de archivos y claves de cifrado de claves maestras de clientes, ya que las redes pueden ser protegidas por claves simétricas se debe generar una pareja de claves por

cada par de nodos $N = \frac{n(n-1)}{2}$ y para las protegidas por claves asimétricas una pareja de claves por cada nodo $N = 2n$, esto permite cierto nivel se seguridad sobre todo para los ataques dentro de una entidad. Hay que tener claro que existen claves que no pueden ser modificadas fácilmente las cuales se denominan estructurales y son la de mayor jerarquía, y claves maestras de menor rango que generan otras claves para los departamentos correspondientes, estas también tienen mecanismos de seguridad físicos que se activarán el momento de estar comprometidas, inclusive pueden autodestruirse.

Las claves en muchas ocasiones nacen con un cliente en la red y pueden desaparecer antes de este, para su creación y vida también se gestiona políticas y procesos que permiten tener control en caso de ataques, lo primero que se realiza es dar de alta al cliente luego de verificar su identidad, posterior a esto se genera, instala y valida una clave para el usuario nuevo, esta es almacenada para su uso, esta clave es utilizada por el cliente mientras tenga periodo de validez, sin embargo en caso de que la clave este comprometida se procede a revocar y destruir el almacén de claves para evitar que los atacantes actúen.

2.4 Herramientas de análisis de protocolos

Una herramienta de análisis de protocolos es software dedicado a monitorizar y capturar tráfico que fluye por la red en un determinado punto, para luego analizar su estructura y componentes, que posteriormente permitirán ya sea a un administrador de redes o a un usuario conocer su función, arquitectura y posibles vulnerabilidades para establecer seguridades, a estas herramientas se las conoce como sniffers (palabra registradas por Network Associates, Inc.).

Analizar protocolos quiere decir reconocer sus partes, su sistema de reglas en forma individual, su funcionamiento, vulnerabilidades y su contenido al transportar información, de ahí que su estructura en si es reconocida como cabecera de protocolo en la cual se encuentran establecidas cada una de sus componentes y el contenido transportado de acuerdo a las capas ya sea modelo OSI o Modelo TCP a la que pertenezca.

Vulnerabilidad quiere decir errores de seguridad localizados en un sistema determinado ya sea por activación de procesos al ejecutarse un protocolo, huecos que quedaron al ser diseñados los sistemas, o puertos que quedan expuestos después de ser utilizados, al ser detectados por programas que escanean vulnerabilidades en los sistemas pueden ser aprovechados por personas interesadas en esos errores para posteriores ataques.

Existen varias herramientas de análisis de tráfico y protocolos que localizan vulnerabilidades y si ya son conocidas se pueden corregir para evitar ataques o buscar alternativas para evitar que queden expuestas, de estas se encuentran licenciadas y opensource, las cuales tienen sus ventajas y desventajas al ser utilizadas, a continuación se menciona las herramientas más comunes con sus características y se establecerá las más apropiadas para ser utilizadas.

2.4.1 Herramientas de análisis de tráfico:

2.4.1.1 Tcpdump

Es un analizador de paquetes que se ejecuta en modo consola. Posibilita al usuario interceptar y visualizar paquetes TCP/IP, y otros que estén siendo transmitidos o recibidos

en una red a la cual la computadora se encuentra conectada. Se distribuye bajo la licencia BSD (Berkeley Software Distribution), siendo un software libre y de código abierto (SLCA). Funciona en la mayoría de los sistemas operativos: Linux, Microsoft Windows, Solaris, BSD, Mac OsX, HP-UX y AIX, entre otros. Emplea la librería Libpcap para capturar paquetes y WinDump para Windows. Se puede utilizar también en el entorno inalámbrico, lo interesante de esta herramienta es que permite aplicar filtros para seleccionar paquetes que se está buscando, sin embargo si no se los quiere aplicar el adaptador tomará todos los paquetes que fluyen en ese instante por la red, además tiene características adicionales que le permiten ser una herramienta poderosa como son:

- Depura aplicaciones que utiliza la red para la comunicación
- Se puede depurar la red en la que se ejecuta.
- Puede capturar y leer datos enviados por otros nodos hacia la red, en el caso de telnet o http no cifra los datos para enviar con lo cual se puede obtener contraseñas u otro tipo de información importante. (Jimenez, 2013)

2.4.1.2 Wireshark.

Es un analizador de protocolos open-source disponible para plataformas Windows y Unix, conocido originalmente como Ethereal, su principal objetivo es el análisis de tráfico además de ser una excelente aplicación didáctica para el estudio de las comunicaciones y para la resolución de problemas de red, se puede considerar que es la herramienta más completa para analizar protocolos y tráfico y es considerada la principal enemiga de los entornos corporativos.

Wireshark implementa una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados; y todo ello por medio de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados.

Se puede decir que wireshark conoce y entiende la estructura de la mayoría de los protocolos, podemos visualizar los campos de cada una de las cabeceras y capas que componen los paquetes monitorizados, proporcionando un gran abanico de posibilidades al administrador de redes a la hora de abordar ciertas tareas en el análisis de tráfico, en el caso de no disponer de la documentación de protocolos para que esta herramienta funcione se puede apoyarse en ingeniería inversa, en muchos casos se puede hacer uso de herramientas de detección de ataque pero si se necesita analizar trafico profundamente del entorno y en tiempo real estas herramientas no son muy efectivas, tomando en cuenta la flexibilidad de un analizador de tráfico sobre todo si se tiene en claro en que parte de la red comenzar dicho análisis.

Para utilizar esta herramienta existen muchos tutoriales en la web, desde su instalación hasta su análisis profundo, sin embargo una gran desventaja es que, el administrador de la red debe tener conocimiento profundo acerca de redes y convicción de autoeducación ya que de no disponer de estas características, esta herramienta sería una aplicación más, como ventaja se puede describir que si se trata de un administrador que necesita analizar tráfico que considere comprometido puede colocar el software en cualquier parte de la red siempre y cuando disponga de los permisos correspondientes y como gran punto a favor es que puede

analizar toda la red sin problemas y tomar las acciones necesarias, en cambio para un atacante es un gran dilema ya que si se conecta remotamente debe lograr que el tráfico deseado esté disponible en el punto en el que ejecuta, de ser una red configurada por segmentos, VLANs y que dispone de ACLs no podría interceptar el tráfico con facilidad. (Borja Merino Febrero, 2011)

2.4.1.2 Kismet

Es un sniffer, un husmeador de paquetes, y un sistema de detección de intrusiones para redes inalámbricas (WLANs) mediante la utilización de tarjetas wireless. Kismet funciona con cualquier tarjeta inalámbrica que soporte el modo de monitorización raw, y puede rastrear tráfico 802.11b, 802.11a y 802.11g. El programa corre bajo Linux, FreeBSD, NetBSD, OpenBSD, y Mac OS X. Se puede operar en Windows, aunque la única fuente entrante de paquetes compatible es otra sonda, kismet puede verificar que la red este bien configurada y puede trabajar en modo monitor, detecta otras redes que estén causando interferencia en la nuestra, si existen APs a nuestro alrededor, los detecta, muestra información de los clientes conectados en la red, permite verificar que tipo de seguridad dispone la red (WEP, WPA, etc.), permite el funcionamiento con la tarjeta en modo monitor y luego guarda un archivo con los paquetes capturados. Es un software fácil de configurar sin embargo los usuarios deben conocer a fondo compilación e instalación de software bajo Linux principalmente ya que en este sistema operativos dispone de todo su potencial. (Dragorn, 2004)

2.4.1.3 NetworkMiner

Es una herramienta de análisis forense de redes y que corre principalmente en plataformas Windows, aunque con el empleo de Mono, puede igualmente hacerlo en distribuciones de Linux. Su propósito es recopilar información sobre los hosts en lugar de recoger información concerniente al tráfico de la red, utilizando como ventaja que el programa no genera tráfico en tiempo real sino que permite hacer un análisis de datos capturados anteriormente ya sea por el mismo programa o por otro. Utilizada tanto en redes cableadas como en inalámbricas, permite ser usada como sniffer pasivo y analizar capturas en formato pcap. Emplea la biblioteca de captura de paquetes estándar Winpcap, que debe estar instalada en la computadora para su funcionamiento. La vista de la interfaz de usuario principal está centrada en el host, NetworkMiner muestra los equipos detectados usando un árbol jerárquico desplegable, observándose todas las direcciones IP involucradas con la red de comunicaciones, al mismo tiempo que muchos otros detalles: dirección MAC, nombre del host, sistema operativo, TTL (time to live), y cuánto tráfico ha sido enviado hacia y desde la dirección. La identificación del sistema operativo puede realizarse apoyándose en las bases de datos Satori, p0f y Ettercap, estas características permiten que el programa detecte fallos en la red o mal uso de esta, o si han sido modificado datos sin permiso, sin que un atacante se dé cuenta que está siendo monitoreado. (Hjelmvik, 2009)

2.4.1.4 Darkstat

Es una herramienta para monitorizar una red, el cual analiza el tráfico de la red y en base a los datos obtenidos genera un informe estadístico en formato HTML. Este informe se puede ver con cualquier navegador. Para este proposito, el autor del programa, Emil Mikulic, ha estado usando el programa "ntop" durante bastante tiempo. Pero no está contento con su estabilidad y su mal uso de la memoria. Por esta razón ha desarrollado "darkstat". Entre las observaciones que realiza el programa, permite: realizar la estadística de direcciones que se generan en la comunicación entre hosts, el tráfico que se produce y los diferentes números de puertos usados por los diversos protocolos. Adicionalmente, el programa permite obtener un breve resumen y gráficos por periodos de tiempo de los paquetes analizados desde que se empieza a ejecutar el programa, esta herramienta se puede utilizar en servidores para conocer su rendimiento en momentos de gran carga de tráfico o al contrario, su forma de realizar el control es a través de la web, en esta se localizan gráficas estadísticas con las cuales se identifica rápidamente información importante para el administrador, el hecho de tener bajo consumo y ver fácilmente las IPs de los equipos con los cuales se encuentra conectado el servidor se puede decir que es muy útil, sin embargo existen herramientas con más capacidades de identificar información. (Knopf, 2005)

2.4.1.5 OmniPeek

Es un analizador de red comercial bastante completo, capaz de realizar capturas en el entorno inalámbrico. Ofrece una interfaz gráfica intuitiva y fácil de usar, se puede utilizar

para analizar con rapidez los paquetes que circulan por la red y solucionar problemas que puedan presentarse en la misma.

Proporciona visibilidad en tiempo real y análisis de la red desde una única interfaz, incluyendo Ethernet, Gigabit Ethernet, 10 Gigabit, conexión inalámbrica 802.11a/b/g/n, VoIP y vídeo. Usando la interfaz de usuario para la visualización de las condiciones de red se pueden analizar rápidamente, profundizar y corregir los cuellos de botella a través de varios segmentos, dispone una interfaz fácil de usar que se vuelve intuitiva para el usuario, proporcionando un análisis experto centralizado para todas las redes bajo administración, además puede visualizarse las características del tráfico, logrando así identificar lo que afecta el rendimiento, dichos análisis se hacen a través de gráficas estadísticas respecto a condiciones de funcionamiento del tráfico utilizando un cuadro de mando interactivo, permitiendo incluso análisis de multimedia, las características de esta herramienta son muy adecuadas para monitorizar tráfico desde el básico hasta estructuras encriptadas muy robustas, sin embargo hay que tomar en cuenta su costo que al final no puede ser tan beneficioso respecto inclusive a sus versiones. (wildpackets, 2012)

2.4.2. Herramientas de análisis de vulnerabilidades

2.4.2.1 NMAP

Es una herramienta de software libre multiplataforma usada para ejecutar la auditoría de las seguridades de las redes evaluando también la seguridad de los sistemas informáticos, con la cual se realiza análisis de cada paquete IP, por lo general los administradores de las

redes llevan adelante inventarios de las mismas ya que NMAP trabaja con información DNS, en la cual se considera el tipo de puerto, protocolos, estados de los puertos y las direcciones MAC que están vinculados a dichos puertos, diseñado para analizar redes grandes rápidamente y para equipos individuales, así como funciona en auditorias de seguridad muchas personas lo utilizan para realizar administración de la red como son: inventarios, actualización de servicios y su actividad.

Sus resultados son salidas en un listado analizado, de esto lo importante son las tablas de puertos, un puerto puede tener tres tipos de estado: estado abierto o estado de escucha, cerrado o estado de no escucha y en estado de filtrado donde el estado del puerto es indeterminado, la tabla de puertos incluye en muchos de los casos detalles de la versión de la aplicación cuando se solicita detección de versiones, además de sus puertos también ofrece información sobre los objetivos analizados por ejemplo el nombre de DNS, listados de posibles sistemas operativos, tipos de dispositivos y direcciones MAC.

Algo importante a destacar acerca de esta herramienta es su capacidad para adaptarse a las condiciones presentes en la red incluyendo latencia y congestión de esta, descubre servidores presentes en la red, puertos abiertos, servicios en ejecución, el sistema operativo en uso y su versión y algunas características de hardware.

Se ha convertido en una herramienta muy utilizada por los administradores de sistemas, siendo usado en pruebas de penetración y seguridad informática, esto también a la ves es una desventaja cuando está en manos de personas que quieren utilizar dichas condiciones para su beneficio ya que NMAP no es detectable fácilmente y fue creado con la finalidad de

evadir IDSs puesto que no interfiere en gran medida con las operaciones de la red y de los objetivos analizados. (Vila & Chica, 2012)

2.4.2.2 NESSUS

Es un escáner de vulnerabilidades muy robusto que está bien adaptado para empresas grandes de redes y funciona a nivel de diversos sistemas operativos, nessus desde consola puede ser programado para escaneos con cron.

En operación normal, nessus comienza escaneando los puertos con nmap o con su propio escáner de puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL (Nessus Attack Scripting Language, Lenguaje de Scripting de Ataque Nessus), un lenguaje scripting optimizado para interacciones personalizadas en redes, opcionalmente, los resultados del escaneo pueden ser exportados como informes en varios formatos, como texto plano, XML, HTML, y LaTeX. Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades.

Actualmente existen dos versiones: "Home" y "Work" Esta última de pago y sin restricciones.

Características:

- Utiliza la arquitectura cliente/servidor. El servidor corre bajo UNIX o LINUX y los clientes en Windows, Java, UNIX por lo tanto es multiplataforma.

- Basa su arquitectura a través de plug-ins.
- Cuenta con su propio lenguaje llamado NASL (Nessus Attack Scripting language) para programar los plug-in, lo que hace sumamente amigable su programación.
- Barrido de puertos e identificación de servicios a través del scanner Nmap.
- Una base de conocimiento muy extensa con las vulnerabilidades descritas en CVE (Common Vulnerabilities and Exposures), con la opción de configurar los parámetros de estas.
- Genera reportes en diferentes formatos como PDF, XML, HTML, texto claro.
- Como parte del reporte nos permite conocer la vulnerabilidad y brinda una unión a la descripción de esta, a su vez propone una solución.
- La opción de verificar varios servidores al mismo tiempo.
- Comunicación segura entre cliente y servidor a través de PKI (Public Key Infrastructure).
- La licencia es GPL (General Public License), que nos permite obtener el código fuente
- Al realizar un escaneo de un sistema objetivo se corre el riesgo de que las vulnerabilidades de NMAP corrompan servicios o sistemas operativos.

(ALBARRAN & GARDUÑO, 2010,pg. 45 - 47)

2.4.2.3 Metasploit Framework

Es una herramienta orientada a introducir exploits (secuencia de comandos utilizada para aprovechar una vulnerabilidad) (Wikipedia.org, 2015), durante un ataque para aprovechar vulnerabilidades de un sistema.

Metasploit utiliza gran cantidad de datos para la ejecución de los ataques porque almacena en el sistema operativo todos los exploits conocidos hasta la fecha, por lo tanto Metasploit para gestionar todos los exploits, módulos y auxiliares utiliza una base de datos en postgresql, no solamente para realizar estas actividades, también para almacenar los ataques y escaneos por el tiempo que dura el proceso de explotación.

La forma como Metasploit trabaja es mediante el uso de dos tipos de códigos, el primero son los exploits exclusivos para cada vulnerabilidad y plataforma, el segundo código son los payloads utilizados después de que el exploit tuvo éxito en quebrantar la vulnerabilidad el cual realiza la tarea de penetrar en el sistema afectado, es decir el exploit lo único que realiza es aprovecharse de la vulnerabilidad y quebranta la seguridad pero deja un camino abierto, el cual es utilizado por el payload para ingresar al sistema operativo con el fin de ejecutar comandos o acciones en la máquina vulnerada bajo el control del atacante informático.

Metasploit utiliza comandos propios para la configuración de las opciones de los exploits, los comandos clave son los siguientes:

- Search: Búsqueda de exploit en la base de datos.
- Use: Selecciona el exploit a utilizar.

- Set: Establece los valores a cada una de las opciones que el exploit requiere para operar.
- Exploit: Inicialización del ataque. (BELTRÁN, 2015)

2.4.2.4 Kali Linux (Backtrack)

Es la nueva generación de la conocida distribución Linux BackTrack, la cual se utiliza para realizar Auditorías de Seguridad y Pruebas de Penetración. Kali Linux es una plataforma basada en GNU/Linux Debian y es una reconstrucción completa de BackTrack, la cual contiene una gran cantidad de herramientas para capturar información, identificar vulnerabilidades, explotarlas, escalar privilegios y cubrir las huellas.

Kali Linux es una completa reconstrucción de BackTrack Linux, y se adhiere completamente a los estándares de desarrollo de Debian. Se ha puesto en funcionamiento toda una nueva infraestructura, todas las herramientas han sido revisadas y empaquetadas, y se utiliza ahora Git para el VCS.

- Más de 300 herramientas de Pruebas de Penetración
- Es Software Libre
- Árbol Git Open Source
- Cumple con FHS (Filesystem Hierarchy Standart)
- Amplio soporte para dispositivos inalámbricos
- Parches al Kernel para inyección.
- Entorno de desarrollo seguro

- Paquetes y repositorios firmados con GPG
- Varios lenguajes
- Completamente personalizable
- Soporte ARMEL y ARMHF (Caballero, 2015)

2.5 Redes Neuronales

2.5.1 Neurona

Como ya se mencionó en el capítulo anterior para asegurar el tráfico de una red con un antivirus o un firewall no es suficiente, además de que este tipo de software debe constantemente estar actualizándose sea privativo u OpenSource y que la red debe estar siendo monitoreada las 24 horas del día por el administrador, cosa que no se lograría fácilmente, es importante un mecanismo adicional que permita a la red monitorearse por sí sola, actualizarse en caso de ataques nuevos que actúen rápidamente en el momento que está siendo identificado el ataque y tomar decisiones sin esperar resultados burocráticos que muchas veces finalizan en desastres.

Tomando en cuenta el diseño de los cerebros humanos y animales se crea las redes neuronales artificiales (ANN), buscando simular las neuronas que disponen estos con las características de aprendizaje, clasificación y adaptación a los problemas que se plantean, Figura 22, procurando que cada parte de una neurona sea recreada con la mayor similitud incluyendo los procesos que realiza al transmitir información, sin embargo el mayor desafío

es diseñar el aprendizaje mediante repeticiones de tareas que una neurona cerebral lo realiza con facilidad.

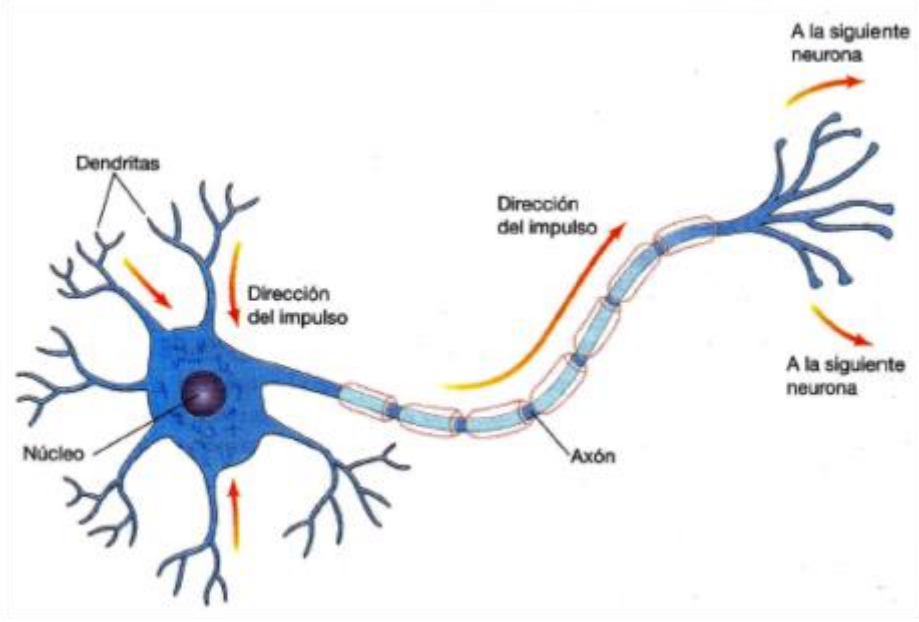


Figura 22: Estructura de una neurona cerebral
Fuente: (Barrero, 2014)

Para que estos procesos sean exitosos cada neurona debe reaccionar a un estímulo eléctrico sobre un umbral de voltaje específico que proviene de otra neurona que de igual manera recibió anteriormente dicho estímulo por medio de su axón a los terminales, a la vez estos se conectan con otros mediante la sinapsis para llegar a otras neuronas.

Las neuronas realizan todo este trabajo basado en el tiempo en milisegundos 10^3 con conexiones sinápticas aproximadamente de 10^{13} individualmente, lo que resulta lento en comparación a los chips de silicio que funcionan en el tiempo basado en nanosegundos 10^9, siendo más lentas para procesar con compuertas lógicas, sin embargo esta lentitud es compensada con las miles de neuronas que actúan sobre un determinado problema para

resolverlo, tomando en cuenta que los procesos que realizan las neuronas no son lineales como los chips de silicio, esto quiere decir que todo el trabajo lo realiza en forma paralela lo que da gran ventaja en comparación con los procesos computacionales ya que si en un sistema neuronal existe la falla de una o varias neuronas dicho sistema no se interrumpe, continua sus labores casi con las mismas características que en un inicio, por ejemplo: En el caso de un computador que ha mantenido funcionamiento por mucho tiempo, el hecho de que tiene procesos lineales no permite en ningún instante descargar sus medios de transmisión y comunicación, por el uso excesivo provocan que si llegase a fallar dicho medio, todo se queda interrumpido inmediatamente o a la ves permite el paso de información sin ser filtrada, es de imaginarse si dicho computador es un controlador de tráfico de red y este falla permitiría que todo tipo de datos pasen, más peligroso aún si no existe un control sobre este durante periodos de tiempo en minutos cualquier ataque a la red puede actuar con libertad sabiendo que estos procesos ofensivos necesitan espacios muy pequeños de tiempo para llevar a cabo sus objetivos, dentro de esta estructura no hay un aprendizaje acerca de estas fallas, así se colocaran varios computadores no hay adaptabilidad al medio fácilmente, menos aún aprendizaje acerca de los problemas, todo esto lo tendría que realizar el ser humano todo el día, he ahí la gran diferencia entre las neuronas y los chips de silicio con grandes velocidades, adicionando que cada neurona suma los INPUT(entradas) de otras neuronas de forma espacio-temporal Figura 23, para establecer su umbral y activar la sinapsis.

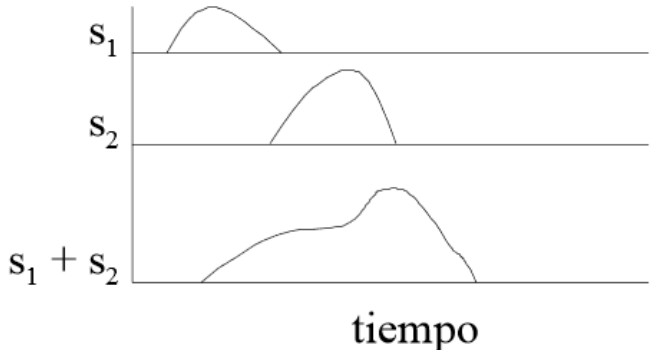


Figura 23: Suma de entradas de dos o más neuronas a una nueva.

Fuente: (Arredondo, 2012)

2.5.1.1 Sinapsis

Las neuronas envían sus salidas por impulsos periódicos (potenciales de acción) desde el soma de la célula propagándolos a través del axón, de ahí estos llegan a las dendritas donde se origina la sinapsis, siendo esta la interconexión entre dos neuronas, la una con un botón sináptico que dispone de vesículas generando la sinapsis química que llega mediante una señal eléctrica pre-sináptica, luego las vesículas se rompen donde se libera una sustancia llamada neurotransmisor el cual es captado por la dendrita estimulándose la emisión de un nuevo impulso eléctrico post-sináptico Figura 24, algo que hay que tomar muy en cuenta y que ayuda mucho al desarrollo de este documento es que el impulso de salida de la sinapsis no es igual al de entrada, estos dependen de la cantidad del neurotransmisor el cual cambia durante un aprendizaje y aquí es donde se almacena la información, la sinapsis es donde se cambia el pulso para debilitarlo o reforzarlo.

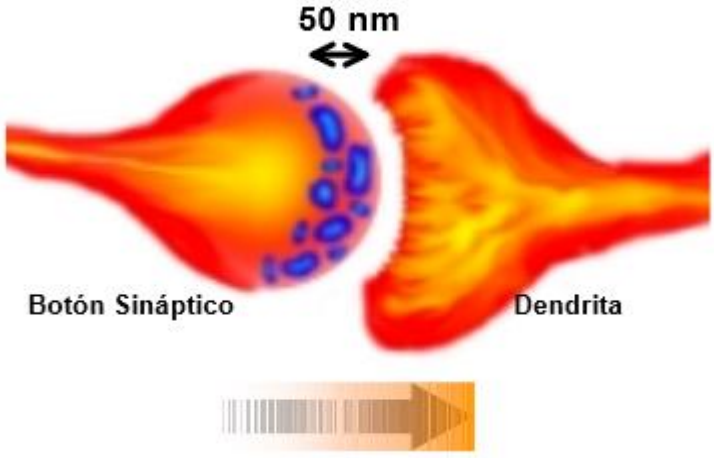


Figura 24: Proceso sináptico de una neurona biológica

Fuente: (Izaurieta & Saavedra, 2006)

En el soma de la neurona se suman las entradas de las dendritas las cuales si llegan a sobrepasar un umbral entonces abra la transmisión del pulso por el axón, posteriormente a la transmisión, la neurona se polariza, en este momento las membranas y las bombas de sodio y potasio paran de actuar, la membrana cambia de estado y se vuelve más permeable al ion positivo y al entrar a la neurona cambia de potencial a través de la membrana neuronal, posterior a esto comienza un periodo refractario de ~ 1ms en el cual los canales de transmisión se cierran, la membrana vuelve a ser permeable, las bombas se activan y la neurona vuelve a su estado inicial, en este periodo la neurona no es susceptible a estímulos sinápticos, estos procesos son las metas a cumplirse por las Redes Neuronales Artificiales. (García F. , 2005)

2.5.2 Modelo Neuronal

La red neuronal parte desde la creación del primer modelo conexionista presentado por McCulloch y Pitts el cual dispone de las entradas excitatorias (x) que serían las señales provenientes de un axón, pesos (w) para las entradas los cuales serían adaptables como sinapsis para reforzar o debilitar una señal y así alcanzar el umbral, esta recibe las suma de las entradas multiplicadas por los pesos correspondientes $\sum xw$, la función (f) sea esta de escalón, lineal, sigmoidea o gaussiana en la cual se supera el umbral, y por último la salida de la función habiendo superado como 1 o como -1 el umbral, siendo esta una estructura conocida como perceptrón Figura 25.

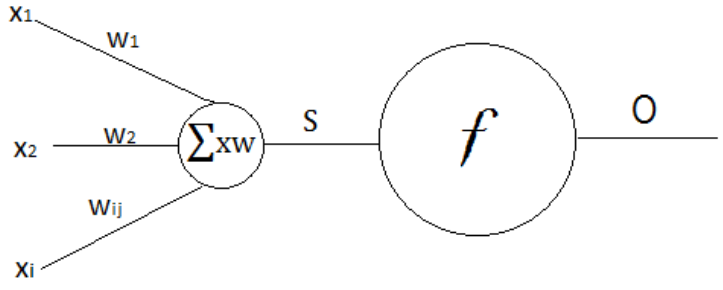


Figura 25: Estructura de una neurona conexionista

Fuente: Elaborado por autor

Al tener entradas de diferentes axones la neurona recibe dichas entradas y las multiplica con los pesos respectivos para reforzar la señal o debilitarla y a estos los suma, posteriormente se activa el umbral dependiendo del tipo de función que se utiliza Figura 26, de acuerdo a esto se modifica el valor del umbral procurando que sea más complicada su activación, pero es problemático ya que se tendría que estar cambiando a cada momento

estos valores, por lo que se recomienda utilizar una neurona de inclinación Figura 26 ya que es más práctico.

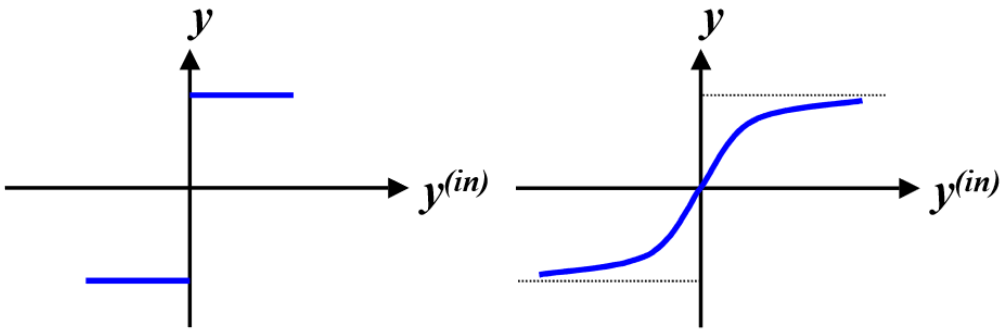


Figura 26: Estructura de función de escalón y sigmoidea

Fuente: (Izaurieta & Saavedra, 2006)

No se puede tener una función estándar para las ANN ya que estas pueden ser de diferentes aplicaciones en las cuales las funciones operan en forma distinta en muchos campos.

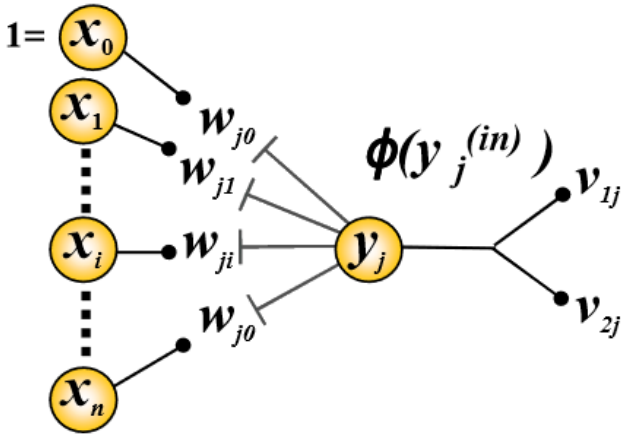


Figura 27: Esquema de una neurona con inclinación

Fuente: (Izaurieta & Saavedra, 2006)

La principal desventaja de las ANN es que constituyen un modelo no descriptivo, esto quiere decir que actúan como una caja negra sin que se pueda conocer la razón de la decisión tomada.

2.5.2.1 Elementos de una Red Neuronal Artificial

2.5.2.1.1 Unidades de proceso

Las unidades de proceso especifican principalmente la estructura de las neuronas para recibir información, clasificarla de acuerdo a su interés y dar resultados, en este caso estaríamos hablando de las entradas que provienen de otras neuronas a través de su axón o de la información que recibe de una red informática, las capas de las cuales está compuesta, tomando en cuenta que puede ser una o varias capas ocultas de acuerdo a lo complicado de su problema a solucionar y las salidas una vez procesadas mediante las funciones y pesos sinápticos para enviarlas fuera de la red.

2.5.2.1.2 Estado de activación

En esta parte se analiza su activación de acuerdo al modelo de red a utilizar ya que en algunos casos depende de un vector en un determinado tiempo, estos estados pueden ser; continuos o discretos, limitados o ilimitados, si son discretos toman valores binarios cero en estado inactivo o uno en estado activo, pero en otros modelos de red con función sigmoidea en cambio se pueden tomar valores 0 y 1 o -1 y 1.

2.5.2.1.3 Función de salida o transferencia

Especifica el tipo de función que utiliza una neurona y que está asociada a la combinación de los pesos y las entradas que proporciona una señal de salida una vez superado el umbral, estas funciones están adaptadas a las neuronas de acuerdo a la tarea a realizar por dicha neurona pudiendo ser: función escalón, función lineal y mixta, función sigmoideal o función gaussiana, cada una de estas con sus características de activación correspondientes para separar la información de acuerdo a las necesidades de la red.

2.5.2.1.4 Conexiones entre neuronas

Para que una neurona pueda intercambiar información con otra, realiza el proceso de comunicación mediante las conexiones entre estas, siendo la entrada total o neta la suma del producto de las señales entrantes por los pesos o sinapsis de aprendizaje, mediante esto la red adquiere conocimiento y a esto se lo conoce como red de propagación. Se utiliza una matriz con los pesos w, si w es positiva indica que la señal es excitadora es decir que la neurona que reciba la señal se activará, pero si w es negativa indica que la señal es inhibidora entonces si la neurona que recibe la señal esta activada enviará una señal para desactivarse, sin embargo si wij (i=emisor, j=receptor) es cero significa que no hay conexión, de ahí que la función de activación entre del producto de las entradas y los pesos produce un nuevo estado de activación de acuerdo a las funciones mencionadas anteriormente, sigmoideal siendo la más utilizada, de esto se deriva que el aprendizaje de las ANN depende de los pesos a los cuales llego la red luego de ser modificados hasta conseguir el peso ideal para resolver

el problema, en otras palabras quiere decir que se modifican los pesos tantas veces sean necesarios hasta obtener lo requerido y de aquí estos quedan estáticos hasta que tenga nuevas entradas para volver a ser modificados con lo cual la red a adquirido conocimiento.

Cuando las salidas una red de neuronas pueden ser conectadas como entradas de niveles previos o del mismo nivel, incluyéndose a sí mismas la red es de propagación hacia atrás.

2.5.2.2 Características de las Redes Neuronales Artificiales

2.5.2.2.1 Topologías

Estas indican la organización y disposición de las neuronas para formar la estructura de la red tomando en cuenta las capas con las que dispone, el número de neuronas utilizadas, su grado de conectividad y el tipo de conexiones, siendo estas:

- Monocapa: teniendo una sola capa en toda la red, esta suele ser utilizada para autoasociación (información incompleta), estableciéndose conexiones laterales, cruzadas o autorrecurrentes.
- Multicapa: dispone de varios niveles o capas las cuales pueden estar conectadas como redes de propagación directa o red de propagación hacia atrás, pudiéndose identificar los niveles desde su entrada de datos hasta su salida.

2.5.2.2.2 Mecanismos de aprendizaje

Son procesos que sigue la red para modificar sus pesos de acuerdo a la información de entrada, estas modificaciones pueden servir para creación, modificación o destrucción de las conexiones entre neuronas, el crearse una conexión significa que el peso de esta es diferente

de cero, al contrario que cuando se destruye, el peso de las conexiones se hace cero, y mientras los valores son modificados la red está aprendiendo, cuando los valores de los pesos se mantienen estables quiere decir que la red ha logrado su aprendizaje, las reglas de aprendizaje se diferencian debido a que si la red realiza su aprendizaje durante su funcionamiento o para este se debe desconectar la red, esto quiere decir aprendizaje con y sin supervisión.

- Aprendizaje con supervisión: es un entrenamiento que tiene la red mediante un agente exterior (supervisor) que le indica la respuesta que la red debe tener luego de una entrada determinada, de no coincidir la respuesta con la que el supervisor necesita obtener se procede a modificar los pesos, esto se realiza hasta que la respuesta de la red coincida o se aproxime a la desea el supervisor, estos aprendizajes se basan en tres tipos de respuestas y su modificación:
  - Corrección de error: se ajustan los pesos en función de la diferencia de los valores deseados y los que fueron proporcionados por la red.
  - Por refuerzo: utiliza un mecanismo de probabilidades para ajustar los pesos, durante el entrenamiento no se indica la salida que se desea de la red, el supervisor solo proporciona una señal de refuerzo a la salida, la cual indica si esta se ajusta a la deseada mediante +1 (éxito) o -1 (fracaso).
  - Por procesos estocásticos: En estos se realizan cambios de los pesos en forma aleatoria para luego evaluar sus efectos a partir de la salida deseada con distribuciones de probabilidad.

- Aprendizaje sin supervisión: en este tipo de redes no existe alguna influencia del exterior para modificar los pesos de las conexiones entre las neuronas que le indique si las salidas son correctas o no, provocando múltiples posibilidades en cuanto a su interpretación, las salidas pueden ser interpretadas en algunos casos como el grado de familiaridad entre las entradas e información mostrada en anteriores casos, en otros caso puede darse la información de entrada codificada para posteriormente presentar de igual forma salida codificada con menos datos pero con la información relevante, o por último puede darse el caso de que se haga un mapeo de características y que a la salida puede presentar una disposición geométrica representando un mapa topográfico de las características de datos en la entrada, de tal manera que si en el futuro se presentan datos similares las neuronas puedan afectar las próximas salidas, a continuación se presentan dos tipos de aprendizaje no supervisado:
    - Aprendizaje Hebbiano: Este aprendizaje ajusta los pesos de acurdo a la relación que tienen las unidades, si estas son positivas se refuerza la conexión, pero si son positiva – negativa, se debilita la conexión.
    - Aprendizaje competitivo y cooperativo: existe competencia entre neuronas para realizar tareas, sin embargo durante esta competencia también estas se colaboran entre sí para evaluar una entrada y solo la neurona indicada se active como la ganadora al alcanzar el valor máximo de su respuesta, esto quiere decir que todas las neuronas compiten por activarse.

2.5.2.2.3 Tipos de asociación entre información de entrada y salida

Como es sabido, asociar información quiere decir relacionar ciertos datos de entrada con datos almacenados, comprarlos y si tiene características similares dar respuesta con el coincidente, en este caso las redes neuronales hacen algo parecido pero distribuido en dos partes; Redes Hetero-asociativas, son aquellas en las cuales la asociación se lo hace a través de pares de datos, en este caso si es una entrada (a_i, b_i) entonces al recibir una información de entrada a_i, la red responde con una salida b_i, existen con conexiones feedforward y feedforward/feedback y con conexiones laterales, de igual manera existen redes hetero-asociativas multidimensionales con aprendizaje supervisado y no supervisado, en el caso de las Redes Auto-asociativas, la red aprende determinadas informaciones a_1, a_2, $a_3 \ldots a_n$, en cuanto la red recibe una información de entrada esta relaciona con una autocorrelación respondiendo con un dato almacenado más parecido al dato de entrada, completando información y asociando esta cuando entra distorsionada, se pueden construir con una sola capa y suelen ser laterales o autorecurrentes, pero estas tienen aprendizaje no supervisado.

2.5.2.2.4 Representación de la información de entrada y salida

Esto quiere decir que se clasifican de acuerdo a los datos de entrada que obtienen, pueden ser continuos (entradas analógicas) donde las funciones de activación también son continuos lineal o sigmoideal, o discretos (binarios) que generan de igual forma resultados discretos siendo sus funciones tipo escalón y en casos especiales redes hibridas. (Daza, 2003)

2.5.3 Tipos de redes Neuronales

2.5.3.1 Red PERCEPTRÓN

Es la primera red creada, consistía en la suma de las señales de entrada (*p*) multiplicada por los pesos escogidos aleatoriamente (*w*), convirtiéndolos en una suma neta (*n*), la cual ingresa a una función para comparar un patrón preestablecido, la función recibe señales y si supera su umbral la salida (*a*) de la red sería 1, de no superarlo sería 0, Figura 27., era una red muy sencilla incapaz de distinguir patrones complejos, sin embargo esto iba cambiando a medida que aquella aprendía y modificaba sus pesos en cada aprendizaje, la capacidad de clasificación del Perceptrón frente a patrones aleatorios era muy congruente, pero a medida que se incrementaba patrones para aprendizaje su precisión disminuía, sobre todo cuando se trata de problemas que no sean linealmente separables.

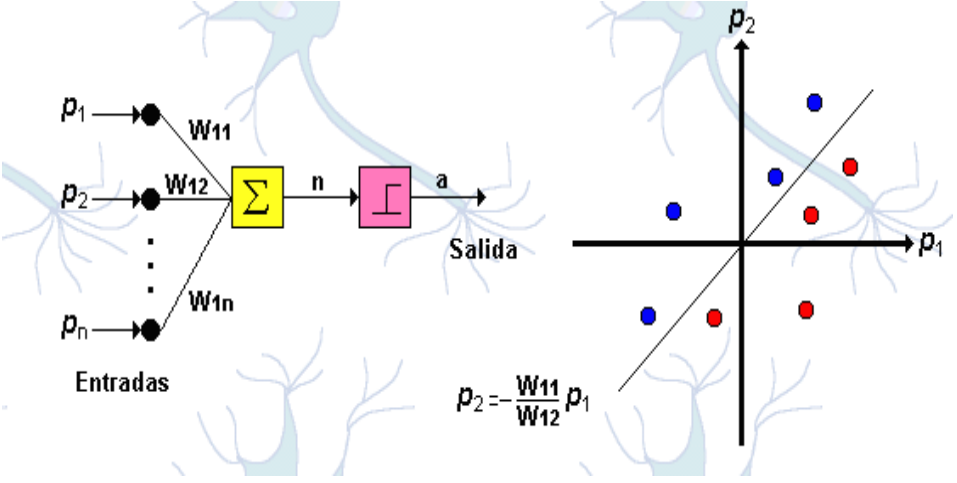


Figura 28: Estructura de una red Perceptrón

Fuente: (Benítez, 2014)

La neurona de salida del Perceptrón realiza una suma ponderada de las entradas por los pesos, resta el umbral y pasa el resultado a una función de transferencia escalón $f(x) = 1$, si $w.x - u > 0$, puede dar 0 en otros casos, la suma ponderada de las entradas debe producir un valor mayor que u para cambiar la neurona de 0 a 1, esta estructura funciona muy bien para problemas de clasificación y se obtiene resultados exactos.

Las funciones de transferencia de la red Perceptrón son hardlim de salidas 0,1 o hardlims de salidas -1, 1, estos se utilizan dependiendo del valor de salida que se espera en la red, sin embargo hay que tomar en cuenta que si una salida es 0 al modificar los pesos multiplicándolos por 0 provoca que un aprendizaje redunde muchas veces hasta encontrar el valor deseado, esto implica un aprendizaje muy lento, por eso la función hardlims es más utilizada.

En muchos casos para facilitar el análisis de comportamiento de una red Perceptrón suelen utilizarse un mapa para las regiones de decisión tomando en cuenta el espacio multidimensional de las entradas de la red Figura 28., clasificándolo de esta manera de una u otra clase separando las regiones por medio de un hiperplano de la cual su ecuación es determinada por los pesos de conexiones y el valor del umbral de la función de activación mediante un algoritmo de entrenamiento, hay que tener en cuenta que los pesos vienen dados por una matriz en forma general en su representación.

$$W: \begin{bmatrix} W_{1,1} & W_{1,2} & W_{1,3} \ldots\ldots W_{1,j} \\ W_{2,1} & W_{2,2} & W_{2,3} \ldots\ldots W_{2,j} \\ W_{i,1} & W_{i,2} & W_{i,3} \ldots\ldots W_{i,j} \end{bmatrix}$$

Si se necesita los pesos para una neurona se representa por un vector compuesto de los elementos de la i-esima fila de W.

$$W = \begin{bmatrix} W_{1,1} \\ W_{2,1} \\ \vdots \\ W_{i,n} \end{bmatrix}$$

De ahí que la función de transferencia hardlim de salida de una neurona, tomando en cuenta que si tiene una sola capa de entrada es limitada a patrones muy sencillos que son linealmente separables y esta quedaría asi:

$$a_i = hardlim\ (Wp + b)$$

2.5.3.1 Regla de Aprendizaje de la red Perceptrón

Este tipo de red necesita conocer las repuestas esperadas para cada una de las entradas, lo que quiere decir que es una red con aprendizaje supervisado hetero-asociativa, y está definido por los pares:

$$\{(a_1, b_1), (a2, b_2), (a_3, b_3), \ldots\ldots, (a_n, b_n)\}$$

Cuando el patrón de aprendizaje *p* es aplicado a la red la salida de la red es comparada con un valor esperado *t* y esta salida es determinada por:

$$a = f\left(\sum_i w_i p_i\right)$$

El aprendizaje de la red y su funcionamiento puede determinarse por sus pesos dependiendo de los algoritmos de entrenamiento de la red que se utilicen, *f* es la función de transferencia utilizada esta puede ser hardlim o hardlims.

Para el entrenamiento de una red Perceptrón se utiliza un conjunto de entradas y pesos de la red, los cuales se ajustan de forma que al final se obtengan las salidas esperadas para cada patrón de entrada, si la red no arroja la salida esperada simplemente se procede a modificar sus pesos hasta que estos se estabilicen y la clasificación de la red sea correcta, cada cambio realizado a sus pesos se aproxima a *p* de forma asintótica, esta es la regla de aprendizaje de la red Perceptrón.

De esto se puede resumir que la ecuación que controla el algoritmo de la red Perceptrón es:

$$w^{nuevo} = w^{anterior} + ep = w^{anteior} + (t - a)p$$

Tomando en cuenta que:

- Si la salida deseada es 0 entonces el peso nuevo es igual al peso anterior más el patrón de aprendizaje.
- Si la salida deseada es 1 entonces el peso nuevo es igual al peso anterior menos el patrón de aprendizaje.
- Si la salida deseada es igual a la entrada entonces el peso nuevo es igual al peso anterior.

Ahora si se incluye error a la red con función de transferencia hardlims entonces quedaría:

- Si el error es igual a 1 entonces el peso nuevo es igual al peso anterior más el patrón de aprendizaje.
- Si el error es igual a - 1 entonces el peso nuevo es igual al peso anterior menos el patrón de aprendizaje.
- Si el error es igual a 0 entonces el peso nuevo es igual al peso anterior.

Las ecuaciones presentadas y las funciones de transferencia serán utilizadas de acuerdo al problema de interés que se tenga, pero para que estas funciones tengan éxito se debe conocer si el problema es linealmente separable, de no ser así se convertiría en una limitación de la red.

De igual manera que se explicó la función de la red Perceptrón con una sola capa, se puede decir que si los problemas son más complejos necesitan de más capas de neuronas que permitan resolverlos, en este caso se habla de una red Perceptrón multicapa la cual tiene una alimentación hacia adelante Figura 29., compuesta de varias capas de neuronas entre su entrada y salida y una sola neurona a la salida, que muchas veces sus capas están ocultas, pudiendo tomas decisiones más complejas de igual manera con características de la red de un solo nivel. (Lezcano, 2014)

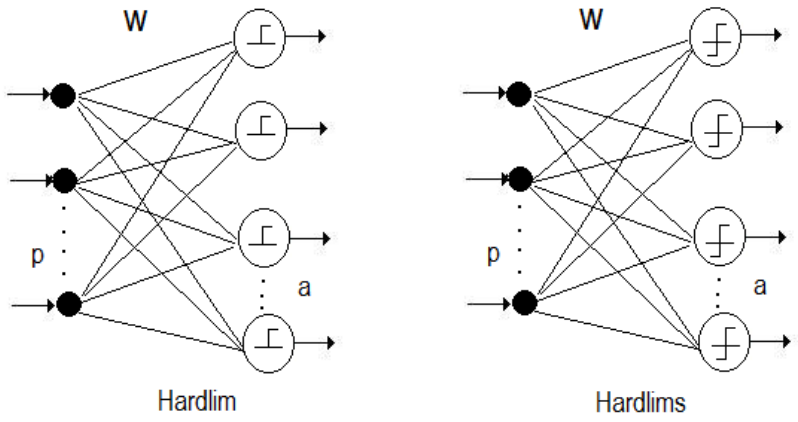


Figura 29: Estructura de las redes Perceptrón multicapa

Fuente: Elaborada por autor

2.5.3.2 Red ADALINE

Esta red fue desarrollada por Bernard Widrow, introduciendo la red Adaline y su algoritmo de aprendizaje LMS (Least Mean Square), esta red es muy parecida a la red Perceptrón, lo que difiere es su función de transferencia la cual es una función lineal, de la misma manera que el Perceptrón la limitación son los problemas linealmente separables pero el algoritmo LMS (regla de WidrowHoff) es más potente que el aprendizaje hardlim, ya que este no es sensible al ruido, y no minimiza el error medio cuadrático; la red Adaline dispone de un solo elemento de procesamiento lo cual provocó que no se la considere como una red neuronal técnicamente, este elemento de procesamiento suma los productos de los vectores de entrada y pesos aplicando una función de salida para obtener un valor, si la suma es positiva la salida será 1, si la suma es negativa la salida será -1, esta salida está dada por la ecuación:

$$a = W^T p$$

Utiliza una función identidad para la activación y como función de salida dando como consecuencia que la salida es igual a la activación siendo la misma entrada neta al elemento.

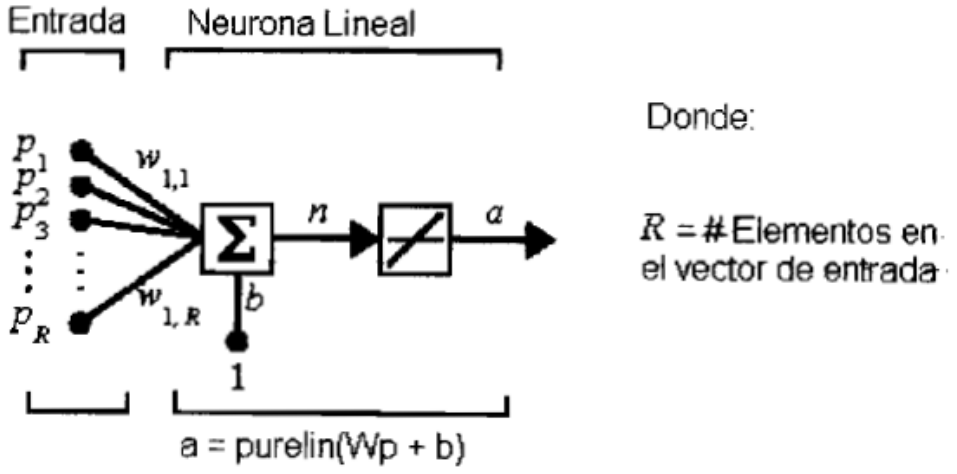


Figura 30: Estructura de una red Adaline

Fuente: (BECERRA, 2001)

Como se mencionó su estructura es parecida al Perceptrón con aprendizaje supervisado, teniendo sus entradas *p* y sus salidas deseadas *t* formando cada par asociado {(p_1, t_1), (p_2, t_2)…(p_n, t_n)} comparándolas a cada salida de la red con el valor asociado *t*, su aprendizaje se enmarca en la corrección de error, para entrenar un Elemento Simple de Procesado, con una función de transferencia lineal Figura 30., lo que busca esta red es modificar los pesos para intentar reducir la diferencia entre la salida deseada y la actual para cada patrón, utiliza el algoritmo de aprendizaje LMS(error cuadrático medio), para los patrones de entrenamiento, tomando en cuenta sus pesos actuales, sus pesos modificados debido a la iteración en los

patrones de entrada, salida y valor deseado, lo que lleva a modificar errores cometidos por la red que serán corregidos gracias al factor de error con sus iteraciones para llegar a la reducción de errores utilizando las variaciones del mismo y estos sean modificados.

En consecuencia debido a las diferencias de la iteración de errores y la iteración de los pesos se obtiene la siguiente fórmula:

$$\Delta e(k) = -\alpha \frac{e(k)p^T(k)p(k)}{|p(k)|^2} = -\alpha e(k)$$

$\Delta e(k)$ Esta es la variación de error que da como resultado al tener iteraciones modificando sus pesos para reducirlo en cada actualización a medida que se presentan las entradas, *e* es el error de la diferencia entre la respuesta deseada *t(k)* y la salida de la red $a(k)=w^T*p$ antes de la actualización, α representa el factor de reducción de error, cada error que se presenta es reducido por este factor α, todo esto se hace hasta que el algoritmo presentado anteriormente alcance convergencia, al elegir α se debe tomar en cuenta que si se elige un valor muy alto al inicializarlo no se estabiliza y se vuelve oscilante buscando permanentemente una actualización a los errores (sobre-corrección), si se escoge un valor muy pequeño en cambio se vuelve lento y tarda mucho en obtener convergencia en los errores, lo cual si se utiliza en un software IDS o IPS tardaría mucho en obtener resultados, ante esto lo más aconsejable es utilizar un valor que se encuentre entre: $0{,}1 < \alpha < 1$, este factor no necesita de la magnitud de las señales que ingresan a la red ya que es auto – normalizado, cada peso que se actualiza ingresa en el mismo momento que los parámetros de entrada en la red y su magnitud es inversamente proporcional a la entrada $|p(k)|^2$, si las

entradas son 1 y 0, no ocurre actualización cuando es 0, en cambio cuando las entradas son ± 1 los pesos se actualizan en cada iteración y su convergencia es más rápida, es por esto que es preferible estas entradas simétricas +1, -1.

De acuerdo a la ecuación proporcionada de $\Delta e(k)$ el cambio del error es el producto negativo de *p(k)* y $\Delta W(k)$, sin embargo como el algoritmo del error cuadrático medio selecciona los pesos de forma colineal entre $\Delta W(k)$ y $\mathrm{p}(k)$ el cambio de error deseado de $\Delta W(k)$ se calcula con el principio de mínima perturbación. De igual manera como se observa en la Figura 30 la estructura de Adaline obtiene valores de actualización de ganancias en cada iteración representadas por la ecuación:

$$b(k+1) = b(k) + \alpha e(k)$$

De aquí que la principal función del algoritmo LMS es corregir errores si todos los patrones de entrada tienen igual longitud entonces la actualización de pesos y ganancias, busca minimizar el error cuadrático medio.

El algoritmo del error cuadrático medio calcula los valores de incremento de $\Delta W(k)$ y $b(k)$ en base a derivadas parciales, para poder localizar el error cuadrático medio se utiliza la gradiente en cada iteración derivando por partes el error con su iteración *e(k)*, respecto a los pesos como a las ganancias obteniendo las fórmulas simplificadas así:

$[\nabla e^2(k)]_j = \frac{\partial_{e^2(k)}}{\partial_{w_{ij}}}$ para j= 1, 2, 3, …. R, derivada respecto a los pesos $\frac{\partial_{e(k)}}{\partial_{w_{ij}}} = -p_j(k)$

$[\nabla e^2(k)]_{R+1} = \frac{\partial_{e^2(k)}}{\partial_b}$, derivada respecto a ganancias $\frac{\partial_{e(k)}}{\partial_b} = -1$

Por último, tomando en cuenta que estas ecuaciones son reemplazadas por la actualización de pesos y ganancias que para calcular el error medio cuadrático es necesario multiplicar el error por el número de entradas obteniéndose que α, se toma como constante al deducir el algoritmo de aprendizaje y su iteración este queda expresado así:

$$W(k+1) = W(k) + 2\alpha e(k) p^T(k)$$

$$b(k+1) = b(k) + 2\alpha e(k)$$

Convirtiéndose de esta manera el error y la ganancia en vectores.

2.5.3.2.1 Aplicaciones de la Red ADALINE

La principal aplicación de la red Adaline es permitir realizar filtros de procesamiento de señales para eliminación de ruido o señales de interferencia tomando en cuenta la suma entre productos a partir de la respuesta de los filtros a la función del impulso unitario y la entrada al sistema, todo este proceso llamado también convulsión de señales para calcular señales de activación de la red y cuanta estimulación recibe esta por parte de una señal de entrada, lo que le permite a la red adapta los pesos para aumentar o disminuir la estimulación que recibirá cada vez que ingrese la misma señal, esta característica viene descrita por la ecuación:

$$y(n) = R[x(n)] = \sum_{i=-\infty}^{\infty} h(i)x(n-i)$$

Siendo *h(i)* la respuesta de los filtros en función del impulso unitario y *x(n)* la entrada al sistema. El problema de esta forma de actualizar los pesos, es que cada vez que se tenga que reprogramar, sobre todo si se realiza filtros digitales con software, la red Adaline no

tendrá la capacidad de especificar la señal de salida deseada en forma automática cuando se le da una señal de entrada específica si el programador no toma en cuenta todas las características de las señales de entrada.

Si se toma en cuenta lo mencionado en los párrafos anteriores y se deduce que para obtener la clasificación que se necesita entre los pesos y los errores con su iteración para ser reducida, esta debe disponer de un vector que se convierte en un filtro adaptativo a las señales de entrada utilizando retardos de línea en un bloque, (Romero M. , 2006), descrita en la ecuación:

$$a(k) = purelin(Wp(k) + b)$$

2.5.3.3 Red BACKPROPAGATION

En las redes anteriores se mencionó que el Perceptrón y Adaline pueden dar solución a problemas que suelen ser linealmente separables, sin embargo cuando no hay esta condición dichas redes no funcionan correctamente, además si ya no se puede reducir los coeficientes de error no podrán clasificar de acuerdo a lo esperado, aquí es donde la red Backpropagation actúa tomando en cuenta que esta aprovecha las características de las redes neuronales al manipular las entradas en forma paralela y la velocidad de los procesadores lineales en cierto momento, la idea es que si se analiza un patrón este posteriormente pueda aprender por sí mismo sin que alguien le dé deduciendo algoritmos correctos, esta será capaz de aprender evitando nueva programación y adaptándose a sí misma para utilizar la relación ya conocida pero nuevos patrones con semejanza a lo aprendido en entornos ruidosos.

Tiene la capacidad de adaptarse al reconocimiento de patrones utilizando propagación hacia adelante tomando en cuenta que el error puede pasar en porciones por las capas de la red y dentro de estas cada neurona clasifica y da resultados a los patrones de entrada para pasar a una nueva capa o a la salida correspondiente dilucidando que en cada paso de patrones las neuronas obtienen una organización y relación de aprendizaje entre estas que a cada momento va reforzándose, al obtener la salida, esta se compara con la deseada calculando el error cometido para luego con este realizar la propagación hacia atrás siguiendo los mismos procesos pero en cada paso de la propagación del error se van actualizándose los pesos de conexión de las neuronas de capas externas u ocultas hasta lograr converger en una clasificación correcta de los patrones de entrenamiento.

La red Backpropagation tiene en su mayoría una estructura multicapa Figura 31, que le permite realizar la clasificación de patrones en varios estados y con aporte de activación de cada neurona.

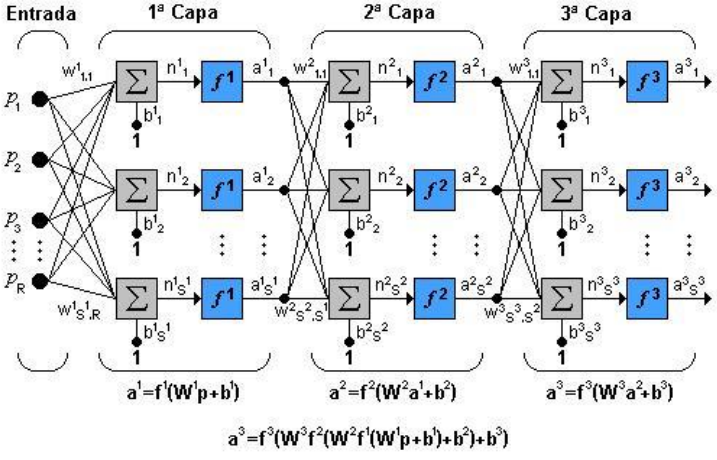


Figura 31: Estructura de la red multicapa Backpropagation

Fuente: (Flores, 2013)

Esta red utiliza características del Perceptrón en forma distribuida tomando en cuenta que la salida de la primera capa es la entrada de la segunda y la salida de la segunda es la entrada de la tercera, cuando la red no es muy grande en muchos casos se suele colocar las siglas S^1:S^2:S^3, cada letra S significa el número de neuronas que contiene cada capa y el número como superíndice representa el número de capa.

Sin embargo cuando las redes multicapa son más grandes no es posible reconocer fácilmente con la nomenclatura mencionada, en estos casos lo más recomendable es utilizar el siguiente esquema:

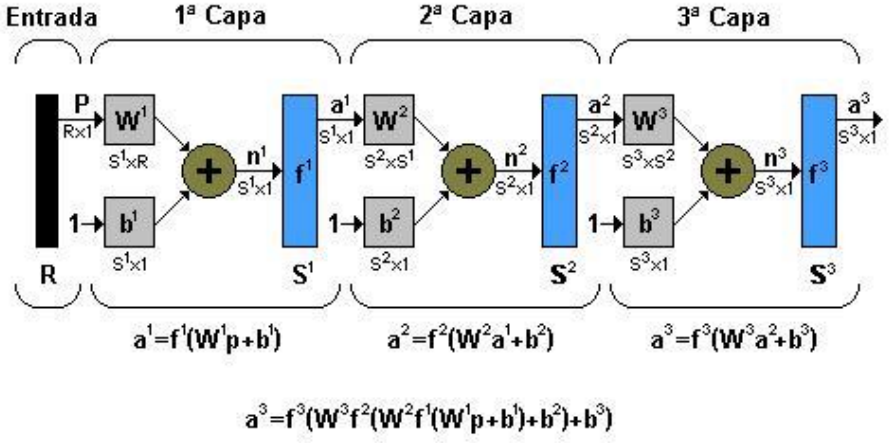


Figura 32: Notación compacta de una red multicapa
Fuente: (Flores, 2013)

2.5.3.3.1 Regla de aprendizaje Backprogation

El algoritmo de aprendizaje de esta red es similar al LMS (error medio cuadrático), siendo esta red previamente entrenada con aprendizaje supervisado, al igual que la Adaline necesita pares de entrenamiento con valores de salida y valores deseados para reducir el error

en cada iteración de aprendizaje. Para realizar el entrenamiento de esta red, es necesario escoger la topología a ser utilizada, esto quiere decir: El vector de entrada con el número de neuronas correspondientes, el número de capas ocultas y las neuronas que disponen en estas, y el vector de salida con sus neuronas correspondientes Figura 32, todo esto dependiendo el problema a resolver, lo que quiere decir es que no se puede tener una cantidad de capas o neuronas predeterminadas para un problema específico, de acuerdo a la topología escogida se colocan los valores iniciales en la capa de entrada.

Al recibir la red el patrón de entrenamiento, este se distribuye a través de todas las conexiones que existan en la topología escogida, creándose una entrada neta *n* para cada una de las neuronas de las capas siguientes, la entrada neta a las neuronas de la siguiente capa se rige en base a la ecuación:

$$n_j^0 = \sum_{i=1}^{q} W_{ji}^0 p^i + b_j^0$$

$$a_k^s = f^s(n_k^s)$$

Donde *0* representa la capa a la que pertenece cada parámetro, *p* es el p–esimo vector de entrenamiento, *j* la j-esima de la neurona oculta, *b* puede ser opcional porque actúa como una entrada más y es la ganancia de la neurona *j* de la capa oculta, W^0 peso que une la componente *i* de la entrada con la neurona *j* de la capa oculta.

El entrenamiento se basa en los siguientes pasos:

- Inicializa los pesos de la red con valores pequeños.
- Se presenta un patrón de entrada y se especifica el valor de salida deseado.

- Se calcula la salida actual de la red

Las salidas de las neuronas de la capa oculta se calculan mediante la ecuación:

$$a_j^0 = f^0(\sum_{i=1}^{q} W_{ji}^0 p_i + b_j^0)$$

f^0es la función de transferencia de las neuronas de la capa oculta.

Se calcula los términos de error para todas las neuronas.

Si la neurona *j* es de la capa de salida, el valor delta es:

$$\delta_{pj}^0 = (d_{pj} - a_j^0) f^s(n_k^s)$$

Esta función debe tener características derivables, pudiéndose utilizarse:

Función Lineal: $f_k(net_{jk}) = net_{jk}$

Función sigmoidal: $f_k(net_{jk}) = \frac{1}{1+e^{-net_{jk}}}$

La elección para este tipo de funciones depende de la representación de la salida, si se necesita que las salidas sean binarias se utiliza sigmoidal caso contrario lineal siendo esta:

$$f_k^{0\prime} = 1$$

Para la función sigmoideal:

$$f_k^{0\prime} = f_k^0(1 - f_k^0) = a_k^s(1 - a_k^s)$$

Quedando los términos de error para las neuronas de salida:

Lineal: $\delta_{pk}^0 = (d_{pk} - a_k^s)$

Sigmoideal: $\delta_{pk}^0 = (d_{pk} - a_k^s) a_k^s(1 - a_k^s)$

En caso de que el error no puede ser derivado directamente en la propagación hacia adelante, este va de regreso por todas las capas que componen la red, denominándose así propagación hacia atrás y regida por la ecuación:

$$\delta_j^0 = f'^0\left(n_j^0\right)\sum_{k=1}^{l}\delta_k^s W_{kj}^s$$

En este caso el error de las capas ocultas depende del error de la capa de salida.

- Por último se actualizan los pesos utilizando algoritmo recursivo desde las neuronas de salida, trabajando hacia atrás hasta la capa de entrada ajustando los pesos en toda la red de la siguiente manera:

Para los pesos de las neuronas de la capa de salida:

$$W_{kj}^0(t+1) = W_{kj}^0(t) + \Delta W_{kj}^0(t+1)$$

$$\Delta W_{kj}^0(t+1) = \alpha\delta_{pk}^0 a_k^s$$

Para los pesos de las neuronas de la capa oculta:

$$W_{ji}^h(t+1) = W_{ji}^h(t) + \Delta W_{ji}^h(t+1)$$

$$\Delta W_{ji}^h(t+1) = \alpha\delta_{pj}^h x_{pi}$$

En los dos casos, se añade el término Backpropagation con un momentum si se desea acelerar el proceso de aprendizaje, basándose en observaciones de la última sección del error cuadrático medio en el proceso de convergencia, pero suavizando mediante un filtro pasa-bajo al sistema para evitar oscilaciones no deseadas.

Como se mencionó anteriormente esta red utiliza el algoritmo LMS como aproximación de pasos descendientes, la única complicación se encuentra en el cálculo de la gradiente, el cual es un término indispensable para realizar propagación hacia atrás con la sensitividad.

Es recomendable colocar valores para los pesos con incrementos pequeños ya que o se sabe en qué momento la gradiente descendiente se encontrará el punto mínimo al cual se encuentra una información local de la superficie, con incremento de pesos grandes se corre el riesgo de pasar por encima del punto mínimo, en cambio con incrementos pequeños la convergencia tardará un poco más pero se evita este inconveniente.

Como ventaja principal se indica que la red Backpropagation es fácil de implementar, siendo muy flexible para su adaptación al aproximamiento de una función, siendo una de las redes multicapa más potentes y una de las más utilizadas, buscando mejorarla a cada momento.

- Todo este proceso de aprendizaje se repite hasta que el término de error:$E_p = \frac{1}{2}\sum_{k=1}^{M} \delta_{pk}^2$ se haga pequeño y sea aceptable para cada uno de los patrones aprendidos. (Valencia, Sanchez, & Yáñez, 2006)

2.5.3.4 REDES NEURONALES SIN SUPERVISION

En las redes presentadas anteriormente se puede observar y concluir que todas estas necesitan disponer de datos con respuestas deseadas para luego ser comparadas con las salidas que obtuvo la red, a esto se le llama aprendizaje supervisado ya que los pesos se ajustan de acuerdo al error cometido por la red al entregar resultados buscando la forma de

reducir el error obtenido entre la salida y los datos que se esperaban. A continuación se presentan otro tipo de redes neuronales que no necesitan conocer los datos deseados esto quiere decir que no es necesario la influencia externa para ajustar los pesos de las conexiones entre neuronas, claro está que estas redes necesitan entrenarse pero esto se realiza a través de presentaciones iniciales, las cuales son almacenadas y en muchos casos categorizadas para luego asociarlas con características que se asemejen a estas o a la ves buscar la categoría a la que pertenecen, con nuevas entradas.

Los algoritmos utilizados para este tipo de redes son:

- Aprendizaje asociativo
- Aprendizaje competitivo

2.5.3.4.1 Redes con APRENDIZAJE ASOCIATIVO

Estas disponen de un vínculo entre las entradas a la red y sus salidas correspondientes, midiendo la familiaridad y extrayendo características de los datos de entrada, siendo las entradas referidas como estímulos y las salidas como respuesta a dichos estímulos; de aquí que basándose en este comportamiento Donald Hebb postula el principio llamado regla de Hebb que dice:

"Una sinapsis aumenta en eficacia si las dos neuronas conectadas por ella tienden a estar activas o inactivas simultáneamente. En caso contrario, la fuerza de la conexión se atenuará" (Lieberman, 2012).

Según la regla de Hebb las actividades que realizan las neuronas antes de la sinapsis y después de esta, marca el camino a fortalecer la conexión de las mismas denominándose mecanismo asociativo pre-post sináptico.

La estructura de estas redes está basada en que la salida de una neurona *a* está determinada a su entrada *p* y de acuerdo a la función de transferencia limitador fuerte Figura 33:

$$a = hardlim(wp + b)$$

En este caso se tomara la entrada *p* como un cero o uno en la cual indica la presencia de estímulo o su ausencia, y el valor de *a* estará limitado por la función de transferencia, en este caso si p = 1, hay presencia de estímulo, si p=0, hay ausencia de estímulo, por el lado de la salida, si a = 1, existe respuesta por parte de la red, si a = 0, no existe respuesta de la red. Al presentarse una asociación de p = 1 y a = 1, será indicada por el valor de *p*, esto quiere decir que la red responderá al estímulo si *wp* es mayor que –*b*.

La red es muy sencilla y responde a dos a dos tipos de estímulos:

Estimulo no condicionado: dispone de una entrada escalar o vectorial que refuerza el aprendizaje y ayuda a hacer la asociación con la salida deseada simulando un real aprendizaje y memorización de la red a los datos presentados, este muchas veces al no condicionar se convierte en una salida deseada de la red.

Estimulo condicionado: en este caso el objeto que se asocia debe ser presentado a la red, la cual la relaciona a la salida deseada de la red, al final siendo posible la entrega de una respuesta correcta con la presentación de este estímulo a la entrada.

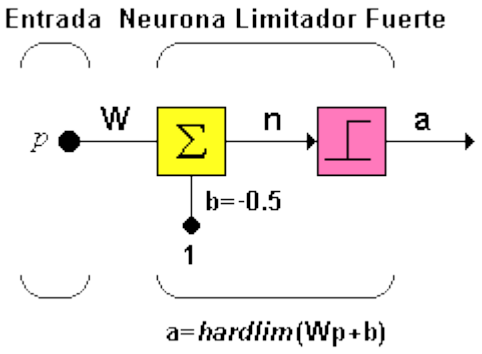


Figura 33: Asociador lineal con limitador fuerte

Fuente: (Acosta, Salazar, & Zuluaga, 2000)

2.5.3.4.1.1 Regla de Hebb

Esta regla indica que si dos neuronas son activadas en cualquier lado de la sinapsis en forma simultánea, la longitud de la sinapsis se incrementará, esto quiere decir por ejemplo que si la entrada p_j produce un valor positivo y la salida a_j produce igualmente un valor positivo, se activa correspondientemente su sinapsis y será $w_{ij,}$ siendo este cambio de peso proporcional al producto de las funciones de activación en cualquier lado de la sinapsis sean estos positivos o negativos produciendo un decremento cuando estos tengan signos contrarios, y reglamentándose en la ecuación:

$$w_{ij}^{nuevo} = w_{ij}^{anterior} + \alpha(a_{iq})(p_{jp})$$

Donde p_{jp} es el j-ésimo elemento del q-ésimo vector de la entrada p_q, a_{iq} es el i-ésimo elemento de la salida de la red, cuando el q-ésimo vector de la entrada es presentado y finalmente α es la tasa de aprendizaje, la cual viene a ser un valor constante y positivo.

Una vez indicada su característica, se puede mencionar que la regla de aprendizaje de Hebb determina el incremento del peso w_{ij} entre la entrada pj y la salida a_j en la q-ésima iteración, está reglamentada por:

$$w_{ij}(q) = w_{ij}(q-1) + \propto a_i(q)p_j(q)$$

2.5.3.4.1.2 Red Instar

Las redes presentadas anteriormente permiten resolver problemas con entradas y salidas escalares, pero en el caso de disponer patrones con entradas vectoriales y salidas escalares para resolver problemas de reconocimiento de patrones es conveniente utilizar una red Instar.

Esta red tiene mucha similitud con el Perceptrón y Adaline respectivamente pero tomando en cuenta que no se analiza sus características de decisión sino que permite reconocer patrones mediante asociación y su aprendizaje no supervisado.

Su ecuación es: $a = hardlims(w^T p + b)$, se activa siempre y cuando el producto entre punto el vector de pesos y su entrada $w^T p$ sea mayor o igual que $-b$, su función va de cero a uno por activación en forma correspondiente.

Hay que tomar en cuenta que esta red se activa cuando el vector de pesos y el vector de entrada apuntan a la misma dirección debiendo tenerse en cuenta que este análisis asume que

los vectores tienen la misma longitud, una de las desventajas de Instar es que los estímulos se deben basar en una iteración constante, caso contrario la asociación se pierde.

2.5.3.4.1.2 Red Oustar

Esta red hace lo contrario que una Instar, tiene una entrada tipo escalar y una salida tipo vectorial, recordando patrones por asociación de un estímulo con un vector respuesta, la misma desventaja que Instar en lo que corresponde a olvido en caso de su aprendizaje con poca iteración.

Está regida por la ecuación: $a = satlins(Wp)$, su función a diferencia de Instar va de -1 a 1 para activación o desactivación a base de la saturación simétrica *satlins*, en algunos casos también la utilizan con hardlims.

2.5.3.4.2 Redes COMPETITIVAS

En estas redes cada una de las neuronas compite y coopera por obtener resultados para resolver una tarea específica tomando en cuenta que una de las neuronas de un grupo determinado en cada capa terminará como vencedora y las otras quedarán forzadas a entregar su valor de respuesta mínimo, especificándose que unas neuronas tienen conexiones de autoexcitación o de inhibición, toda la competencia se basa en la proximidad al patrón de entrada, la más cercana es la ganadora y posteriormente ajusta su peso para aproximarse aún más, a esta neurona se la denomina neurona ganadora toma todo (winner take all), siendo a cada momento más parecida a la entrada. Los datos de entrada que recibe esta red son

categorizados para la activación de la neurona correspondiente mediante las correlaciones entre los datos de entrada.

Estas redes tienen asignado un peso total en las cuales el aprendizaje solo afecta a las neuronas ganadoras en las que se encuentra distribuido el peso entre las conexiones de las cuales se sustrae una parte de los pesos de dichas conexiones para dar a la neurona ganadora, repartiendo igualitariamente entre todas las conexiones que proceden de las unidades activas, dicho de otra manera la variación del peso de una conexión entre la unidad *i* y otra *j* será nula si la neurona *j* no recibe excitación por parte de la neurona *i* y se modificará si es excitada por dicha neurona.

2.5.3.4.2.1 Red de Kohonen

La característica principal de este tipo de redes es que se basa en los mapas auto-organizativos que constan en unidades de proceso compuestas por la organización de neuronas en sus determinadas topologías, esto quiere decir que existen unidades de proceso con estructuras idénticas que se pueden encontrar cercanas entre sí, pero con tareas diferentes gracias a la evolución de dichas unidades en sus parámetros, como ejemplo tenemos la representación de cierto tipo de información en imágenes visuales, abstracciones entre otras, llamando a estas unidades mapas topológicos procurando clusterizar la información con características más relevantes que permita relacionar estas para localizar cierta información requerida, que sean capaces de adaptarse a la información presentada sin necesidad de mecanismos externos que determine la clasificación de la red, según Kohonen ciertas redes

neuronales pueden responder a parámetros de entrada de acuerdo la posición de una neurona (topología).

A partir de los estudios de interacción lateral Kohonen indica que las neuronas más cercanas al patrón de entrada propuesto son las que refuerzan su activación y las alejadas son las que se debilitan a lo mencionado presenta la ecuación como formulación en el campo discreto:

$$\mu_i(t) = \sigma[\theta_i(t) + \sum_{k=_{16}}^{16} \gamma_k \, \mu_{i+k}(t-1)]$$

Donde:

$\mu_i(t)$ es la salida de la unidad i

$\sigma[x]$ es la función de tipo sigmoide

γ_k es el coeficiente de señal de muestreo de la función sombrero mexicano Figura 34.

Acotando a esta ecuación se dice que las neuronas ubicadas con una topología tipo vecindario provocan un función tipo sobrero mexicano a medida que se acercan o se alejan a la entrada específica.

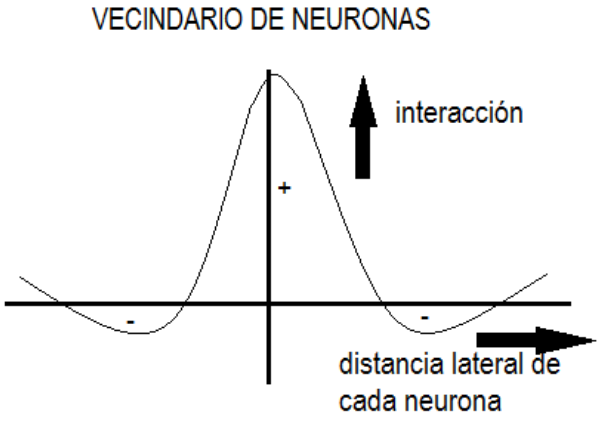


Figura 34: Función tipo sombrero mexicano en la interacción lateral de las neuronas

Fuente: Diseñado por autor

2.5.3.4.2.2 Mapas de Kohonen

Dentro del cerebro humano se ha demostrado que existen organizaciones neuronales predeterminadas genéticamente y otras organizaciones que sean probables que se generen mediante el aprendizaje, siendo entonces el cerebro capas de formar mapas topológicos mediante las informaciones recibidas del exterior, lo que le permite crear y ordenar neuronas o grupos especializados con características de alto nivel.

A partir de lo mencionado Kohonen presentó un sistema con comportamientos similares al cerebro humano buscando demostrar que un estímulo externo por si solo era suficiente para indicar cómo se forman los mapas, teniendo dos variantes LVQ[8](unidimensional) y

[8] Técnica mediante la cual el espacio de entradas es dividida en un número determinado de regiones y cada una de estas está definido por un vector que la caracteriza.

TPM[9](bidimensional o tridimensional) basadas en el principio de formación de mapas topológicos que establecen características comunes de información en las entradas de la red.

A dicho mapa le pone el nombre de mapa de características de Kohonen, siendo este una red neuronal de dos capas: capa de entrada y capa de competición Figura 35.

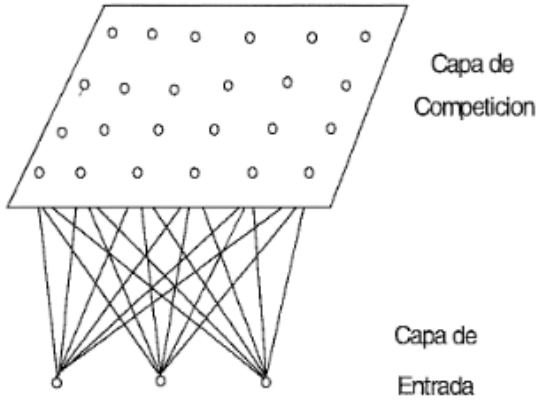


Figura 35: Estructura del mapa de Kohonen

Fuente: (Isasi, 1996)

El mapa de Kohonen utiliza un algoritmo de aprendizaje el cual establece los pesos de las conexiones entre las neuronas de entrada y las de salida, este algoritmo sigue la siguiente cronología:

1. Se inicializan los pesos con valores pequeños, fijándose la zona del vecindario entre las neuronas de salida.

[9] Tipo de red neuronal artificial entrenada utilizando aprendizaje no supervisado que produce una representación discreta del espacio de las muestras de entrada.

2. Se presenta a la red información de entrada en forma de vector cuyos componentes son valores continuos.
3. Se determina la neurona ganadora para cada capa de salida, esta será aquella cuyo vector sea más parecido a la información de entrada, calculándose las distancias entre ambos vectores considerándose una por todas las salidas utilizando la distancia euclidea sin la raíz cuadrada.

$$d_i = \sum_{j=i}^{N} (p_j - w_{ij})^2$$

Siendo:

p_j: el componente i-ésimo del vector de entrada.

w_{ij}: el peso de la conexión entre la neurona *j* de la capa de entrada y la neurona *i* de la capa de salida.

4. Localizada la neurona ganadora se actualizan los pesos de las conexiones entre las neuronas de entrada y dicha neurona, de igual forma entre las neuronas de entrada y las vecinas de la ganadora, asociando la información de entrada con la zona de la capa de salida mediante la ecuación:

$$w(q) = w(q-1) + a(q)\big(p(q) - w(q-1)\big)\ para\ i\ \in X(q)$$

El tamaño de *X(q)* se reduce en cada iteración del ajuste de los pesos con lo cual cada vez que su distancia entre el conjunto de neuronas es menor se dice que estas son vecinas.

El coeficiente de aprendizaje o parámetro de ganancia que tiene un valor entre 0 y 1, decrece con cada iteración en el proceso de entrenamiento, de esta manera que cuando se ha

presentado un número de veces un patrón de aprendizaje su valor es nulo, en este caso el valor de los pesos es prácticamente muy pequeño.

Para encontrar este coeficiente de aprendizaje se utiliza la ecuación:

$$\alpha(q) = \frac{1}{q} \qquad \text{y} \qquad \alpha(q) = \alpha_1(1 - \frac{q}{\alpha_2})$$

Siendo α_1 un valor de 0.1 o 0,2 y α_2 el número total de iteraciones de aprendizaje.

5. Todo el proceso debe repetirse volviendo a presentarse el juego de patrones de aprendizaje hasta obtenerse la salida deseada.

En las redes competitivas, el aprendizaje ocurre cuando una neurona *i* es miembro de un conjunto *X(q),* estas redes tienen similitud con las redes Instar con la diferencia que el aprendizaje no es proporcional a la salida de la neurona *i*, ya que la red de Kohonen se dedica a la clasificación ya que la neurona ganadora que se activa representa a una clase a la cual pertenece una información de entrada y si se le presenta una entrada parecida se vuelve a activar la neurona de salida u otra cercana debido a la semejanza de clases, esta red es utilizada en la mayoría de casos en los que se establece relaciones desconocidas previo a un conjunto de datos. (Isasi, 1996)

2.5.3.4.2.3 Red de Hamming

En las redes competitivas es la de más simple aprendizaje, tomando en cuenta que su estructura es la compleja en este caso, compuesta por una primera capa Instar y una segunda empleando conceptos característicos de una red recurrente Figura 36 la cual permite la competencia entre neuronas, cada neurona de salida de esta red compite una con otra para

determinar la ganadora con la cual se da a conocer el patrón más representativo de entrada, toda esta competición la hace con inhibición lateral mediante un conjunto de inhibiciones negativas entre las neuronas de la capa de salida.

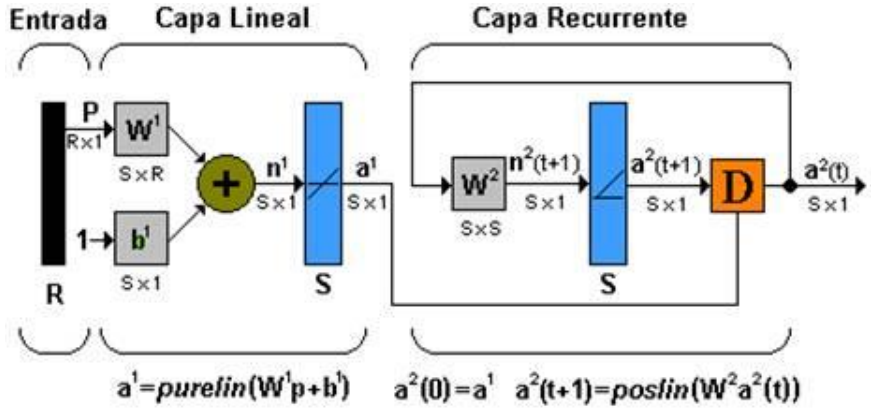


Figura 36: Estructura de la red de Hamming

Fuente: (Flores, Instituto Politécnico Nacional, 2013)

En la capa 1 la red Instar clasifica un patrón, si es necesario la clasificación de múltiples patrones también es necesario múltiples Instar.

Para la capa 1 la matriz de pesos W^1 y el vector de ganancias b^1 son:

$$W^1 = \begin{bmatrix} {}_1W^T \\ {}_2W^T \\ . \\ . \\ {}_SW^T \end{bmatrix} = \begin{bmatrix} P_1^T \\ P_2^T \\ . \\ . \\ P_Q^T 1 \end{bmatrix}, \quad b^1 = \begin{bmatrix} R \\ R \\ R \\ R \end{bmatrix}$$

Con su salida en la primera capa:

$$a^1 = W^1 p + b^1 = \begin{bmatrix} P_1^T p + R \\ P_2^T p + R \\ \cdot \\ \cdot \\ P_Q^T 1 + R \end{bmatrix}$$

Siendo así la salida de la capa 1 igual al producto de los vectores prototipo con la entrada más el vector R, indicando de esta manera que tan cercano está el vector de la entrada a los patrones prototipo, W^1 es el vector prototipo, b^1 es igual al número de elementos de cada vector de entrada *R*, además el número de neuronas *S* es igual al número de vectores prototipo *Q*.

En esta capa 1 la red Instar utiliza la función *poslin* con la cual se decide si el vector de entrada está lo suficientemente cerca al vector prototipo

En la capa 2 esta red competitiva utiliza varias Instar para determinar el patrón prototipo más cercano, cada neurona será inicializada con las salidas de una capa creada como retroalimentación, esta indica la correlación entre patrones de entrada y el vector prototipo, durante esta fase las neuronas compiten entre sí hasta encontrar la ganadora, después de esto solo una obtiene la salida uno la cual indica la categoría de donde salió.

Todo este proceso se resume de la siguiente manera:

- La salida de la capa 1 se utiliza para inicializar la segunda capa.
- La salida de la segunda capa está determinada por una relación recurrente.

- Los pesos para la segunda capa son fijados de tal manera que los elementos de la diagonal sean 1 y los que están fuera tengan valores negativos.
- Se produce una matriz con efecto inhibitorio en la cual la salida de cada neurona tiene efectos inhibitorios sobre el resto de neuronas.

  De los pasos mencionados se obtiene la ecuación:

$$a^2i(t+1) = poslin(a^2i(t) - \varepsilon \sum_{j \neq i} a^2i(t)), \text{ donde } 0 < \varepsilon < \frac{1}{s-1}$$

En cada iteración, existe un decremento en la salida de la neurona proporcionalmente a la suma de la salida de otras neuronas, la salida de las neuronas con valor más alto se decremento más lentamente que otras neuronas.

Estas redes son muy utilizadas por su simplicidad, sin embargo también tienen problemas en determinadas partes como se menciona a continuación:

1. Compromiso entre la velocidad de aprendizaje y estabilidad de los vectores de pesos.
   - El coeficiente de aprendizaje α tiende a cero esto quiere decir que su aprendizaje se vuelve lento una vez que el vector alcanza el centro del clúster[10] en la vecindad este tiene a permanecer siempre cerca del centro.

[10] Conjunto de sectores que componen la vecindad de neuronas, las cuales están constantemente compitiendo por obtener activación, las más cercanas componen el centro del clúster donde se activa la neurona ganadora y las más lejanas componen la interacción lateral en la vecindad, esto significa que las neuronas pueden estar organizadas por categorías.

- Cuando el coeficiente tiende a 1, el aprendizaje es muy rápido, sin embargo cuando se alcanza el clúster el coeficiente continúa oscilando mientras aparecen los vectores.

  Se puede solucionar esto con un valor de α grande para aprendizaje rápido y que se vaya decrementando mientras se avanza en el entrenamiento hasta alcanzar los vectores prototipos estables.

2. Problemas de clasificación cuando los patrones están muy próximos

   Los vectores de pesos pueden ser muy abundantes y el hecho de estar muy cercanos puede contribuir a interrumpir la clasificación de uno y otro.

3. Neuronas muertas

   Al iniciar un vector con pesos puede darse el caso que este comience lejos de los vectores de entrada, provocando que nunca se acerque con lo cual no tendría función alguna, a esto se le llama neurona muerta.

2.5.3.4.2.3 Estructura de las redes competitivas

Las redes competitivas como ya se mencionó están estructuradas a base de regla Instar similar a las asociativas pero con cierto grado de recurrencia, se concentra un grupo de Instar para responder a un grupo de vectores de entrada en diferentes regiones del espacio y clasificarlos, la Instar con mayor respuesta para una entrada es la que identifica que vector de entrada adecuado, esta sería la que tenga su respuesta diferente de cero, compitiendo entre ellas por obtener la activación correspondiente.

En el caso de las neuronas de la segunda capa de la red de Hamming estarán siempre compitiendo porque estas pueden hacer que sus neuronas se activen por sí mismas y terminen inhibiendo al resto, este proceso se lo puede hacer mediante la función de transferencia:

$$a = compet(n)$$

Esta función hace el trabajo de una capa recurrente competitiva, donde *a* es la salida de la red y *n* la entrada neta a la función de transferencia, *compet* es la función de transferencia que localiza el índice de una neurona de entrada neta, la más grande para fijar la salida en uno, ubicando valores cero para el resto de neuronas, igual que en la red de Hamming los vectores prototipo se almacenan en las fila de *W*, la entrada neta n calcula la distancia entre el vector de entrada y cada prototipo tomando en cuenta que los vectores tienen longitudes normalizadas, la entrada neta de cada neurona es proporcional al ángulo formado entre el vector de entrada y el vector prototipo, al remplazar la red recurrente de Hamming con una función de transferencia competitiva se resume en la siguiente ecuación:

$$a = compet(Wp)$$

Esta función de transferencia competitiva asigna el valor 1 a la neurona que tenga un vector de pesos con dirección más cercana al vector de entrada.

El proceso de aprendizaje de las redes competitivas se basa en las reglas Instar, las cuales entrena los pesos de la red sin conocer los vectores prototipo, los mismos resultados se pueden obtener a través de la regla de Kohonen, tomando en cuenta su coeficiente de aprendizaje. Así, las entradas serán clasificadas de acuerdo al número de neuronas creadas, para cada neurona los pesos normalizados son escogidos aleatoriamente, en este caso se

multiplica el vector de pesos por las entradas, el vector de peso de la neurona que tenga el valor con la dirección más aproximada a la entrada será escogida como la neurona ganadora de acuerdo a la ecuación mencionada anteriormente o por la regla de Kohonen:

$$w^{nuevo} = 2w^{anterior} + \propto (p - 2w^{anterior})$$

Donde se toma en cuenta el valor de la tasa de aprendizaje $\propto$ y si se escoge entradas en forma aleatoria y se presenta a la red en cada iteración el vector de pesos *W* se acercará más al vector de entrada *p*. (Calderón, 2003)

2.5.3.4.3 Redes RECURRENTES

En los estudios de las redes anteriores se tomaba en cuenta que estas podían ajustar sus pesos de acuerdo a la asociación en las entradas con las salidas, o competencia de las neuronas por categorías dentro de una vecindad, pero con los problemas de lentitud de aprendizaje u oscilación de los valores una vez alcanzado el peso ideal, teniendo que reafirmar los aprendizajes en cada momento de reducción de error, sin embargo esto es sobrellevar el tiempo a un punto demasiado alto en sistemas lineales el cual es muy inseguro para evitar ataques en periodos cortos, a partir de este tema se analiza el aprendizaje en sistemas lineales y no lineales dinámicos y estáticos con altos grados de recurrencia como modelos recursivos.

Estas redes pueden disponer de ciclos o bucles en las conexiones:

- De una neurona con otra
- Entre neuronas de una misma capa

- Entre neuronas de una capa a una capa anterior

En este tipo de redes se encuentran las redes dinámicas por naturaleza y las redes estáticas que siendo estas multicapa logran comportamientos dinámicos realimentando sus entradas como muestras de las anteriores salidas.

Lo complicado de estas redes es que el hecho de permitir conexiones recurrentes aumenta el número de pesos de la red, su capacidad de representación se incrementa, esto implica que su aprendizaje será difícil ya que todo está gobernado en base al control geométrico diferencial, de aquí que se proponen redes de naturaleza dinámica.

2.5.3.4.3.1 Red de Hopfield

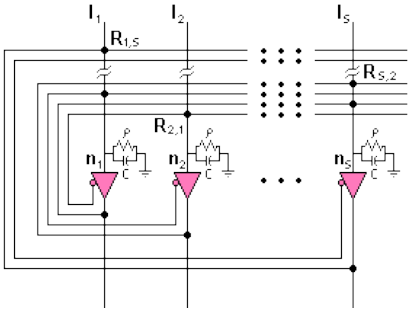


Figura 37: Estructura de la red de Hopfield modelado en circuito electrónico

Fuente: (Acosta, Salazar, & Zuluaga, 2000)

En esta red Hopfield propone toda la red neuronal como un circuito compuesto de amplificadores operacionales como neuronas Figura 37, utilizando adicionalmente una red asociada con capacitancias y resistencias y la ecuación correspondiente que define el comportamiento de dicha red es:

$$\in \frac{d\boldsymbol{n}(t)}{dt} = -\boldsymbol{n}(t) + W\boldsymbol{a}(t) + \boldsymbol{b}$$

La red de Hopfield está compuesta por neuronas dinámicas conectadas todas entre sí utilizando ecuaciones diferenciales no lineales lo que le hace una red con funcionamiento propiamente asociativo que puede reconocer patrones de entrada incompletos y con ruido, lo descrito es a través de la función de Lyapunov aplicado al análisis de las redes recurrentes obteniendo la ecuación:

$$V(\boldsymbol{a}) = -\frac{1}{2}\boldsymbol{a^T W a} - \boldsymbol{b^T a}$$

Esta función no describe un proceso de aprendizaje específico, pero si permite determinar una matriz de pesos mediante su procedimiento de función de alta ganancia, su forma para obtener los pesos $\boldsymbol{W}$ y el vector de ganancia $\boldsymbol{b}$ lo realiza haciendo que *V* tome la forma de una función que se quiere minimizar, convirtiéndolo en un problema de minimización cuadrática ya que la red de Hopfield minimiza a *V*.

La red de Hopfield puede funcionar como una memoria asociativa recuperando información almacenada mediante el uso de parte de su contenido, al presentarse un patrón de entrada este será igual a la salida para posteriormente converger al patrón prototipo más cercano siendo esta una función de Lyapunov[11].

Para establecer que los patrones prototipos son mínimos de la función Lyapunov, se utiliza la siguiente ecuación que evalúa el error de aproximación:

[11] Es una función que demuestra la estabilidad de un punto fijo en un sistema dinámico o en las ecuaciones diferenciales autónomas.

$$J(a) = -\frac{1}{2}\sum_{q=1}^{Q}([p_Q]^T a)^2$$

Si los elementos de *a* se restringen ha ± 1, la función es minimizada en los patrones prototipo asumiendo que estos son ortogonales y evaluando el error en uno de ellos, se tiene lo siguiente:

$$J(a) = -\frac{1}{2}\sum_{q=1}^{Q}([p_Q]^T p_j)^2 = -\frac{S}{2}$$

Por tanto utilizando la regla de aprendizaje supervisado de Hebb para calcular matriz de pesos la función de Lyapunov es:

$$V(a) = -\frac{1}{2}\sum_{q=1}^{Q}([p_Q]^T a)^2 = J(a)$$

Cuando los patrones prototipo son ortogonales cada uno de estos serán un punto de equilibrio de la red procurando evitar los indeseables, para esto el número de patrones almacenados no debe superar del 15% del número de neuronas que se tenga en la red.

Mediante la red de Hopfield y su comportamiento dinámico de las redes recurrentes, estas permiten identificar sistemas dinámicos no lineales, basándose en condiciones estrictas para los pesos de la red por medio de la función de Lyapunov, pero todo esto gracias al algoritmo de Chemotaxis[12] Figura 38, tomando en cuenta que se lo puede hacer sin

[12] Algoritmo utilizado en redes recurrentes que se basa en el movimiento de un organismo en respuesta a un estímulo químico, pero la red de Hopfield lo utiliza para identificación de sistemas dinámicos.

necesidad de calcular la gradiente del error siendo una gran ventaja, el cual toma pesos iniciales al azar con distribución Gaussiana[13] siguiendo una dirección específica cuando las iteraciones son exitosas hasta que la función de error no muestre cambios.

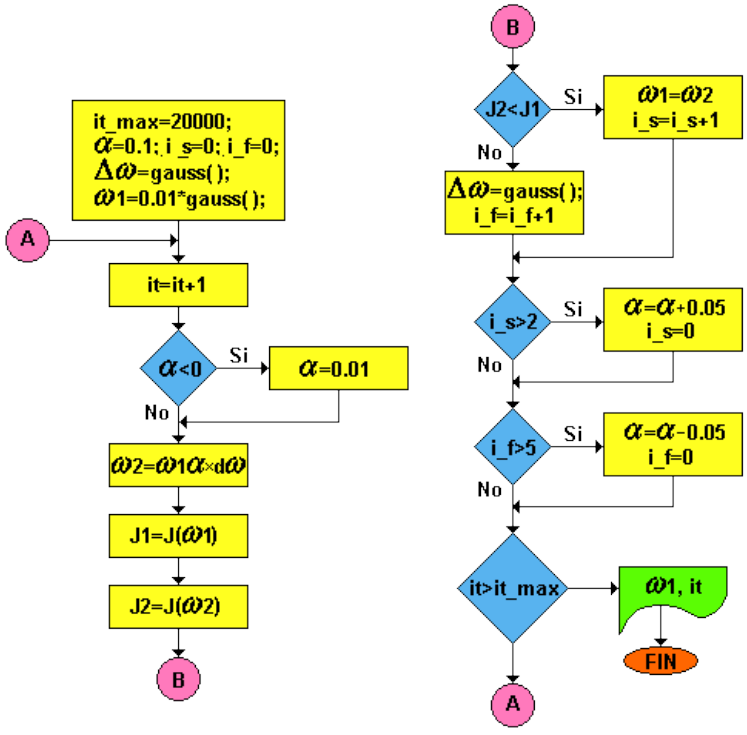


Figura 38: Algoritmo de Chemotaxis

Fuente: (Horat & Cañizales, 2006)

2.5.3.4.3.2 Redes Multicapa

Las redes multicapa son en su mayoría de naturaleza estática como se estudió en la red Perceptrón, para un patrón de entrada se tiene una salida asociada ya que esta no evoluciona,

[13] Herramienta estadística que sirve para calcular la densidad de probabilidad normal para un determinada media y desviación estándar.

pero pueden obtener un comportamiento dinámico realimentando sus entradas con sus salidas.

Esta red se compone de una capa estática, la cual tiene un número de neuronas superior al número de variables de estado del sistema que tiene que identificar, la salida de esta capa se dirige a un sumador en el cual se resta el valor que tenía anteriormente la variable de estado que identifico el sistema Figura 39, de esto se obtiene la derivada de cada una de las variables que identificó el sistema.

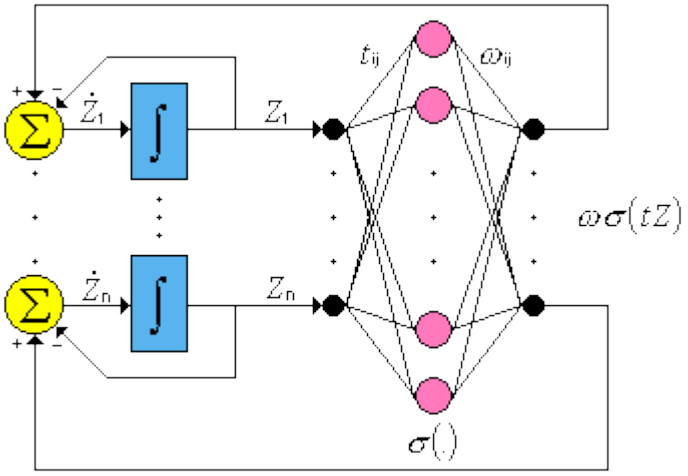


Figura 39: Estructura de una red dinámica multicapa

Fuente: (Acosta, Salazar, & Zuluaga, 2000)

El comportamiento de esta red se describe por la ecuación:

$$\frac{d}{dt}z = \bar{f}(z) = Ax + \omega\sigma(Tz)$$

Para identificar el comportamiento de un sistema autónomo se describe por la ecuación:

$$\frac{d}{dt}x = f(x) = Ax + f_o(x)$$

El entrenamiento de la capa estática se lo realiza mediante el algoritmo de Chemotaxis descrito en la red de Hopfield o el algoritmo Backpropagation, la red luego de ser entrenada se presenta con la siguiente estructura:

$$\frac{d}{dt}\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} -z_1 \\ -z_2 \\ \vdots \\ -z_n \end{bmatrix} + \begin{bmatrix} W_{11} & W_{12} & \cdots & W_{1n} \\ W_{21} & W_{22} & \cdots & W_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ W_{n1} & W_{n2} & \cdots & W_{nn} \end{bmatrix} \begin{bmatrix} \sigma(t_{11}z_1 + t_{12}z_2 + \ldots + t_{1n}z_n) \\ \sigma(t_{21}z_2 + t_{22}z_2 + \ldots + t_{2n}z_n) \\ \vdots \\ \sigma(t_{n1}z_1 + t_{n2}z_2 + \ldots + t_{nn}z_n) \end{bmatrix}$$

Se puede garantizar que la red ha identificado la dinámica del sistema cuando el Jacobiano de la red en el origen obtiene valores propios muy cercanos al sistema aproximado e iguales a los de la red multicapa por medio de la ecuación $J_H = -I_n + WT$, esto se lo hace mediante una transformación de una red dinámica multicapa en una red recurrente tipo Hopfield.

2.5.3.4.3.2 Redes Elman

Este tipo de redes recurrentes está compuesta de dos capas de tipo Backpropagation una capa oculta y una de salida, la capa oculta dispone de una conexión de realimentación hacia su entrada Figura 40, lo cual le permite un aprendizaje de reconocimiento y puede generar patrones que varían en el tiempo.

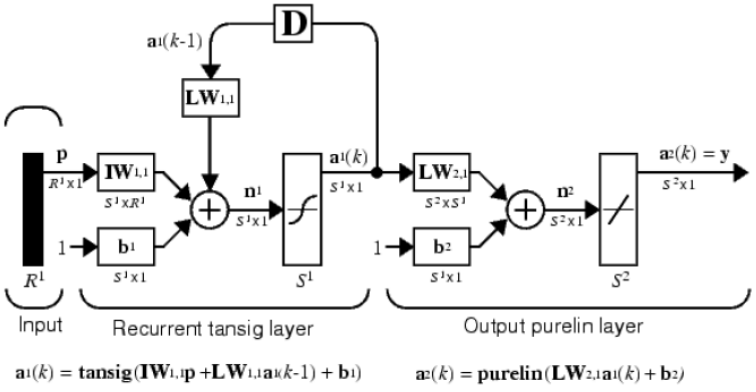


Figura 40: Estructura de la red de Elman

Fuente: (Albanés & García, 2011)

La característica principal de esta red expresada incluso como una ventaja, es que permite gracias a sus funciones, aproximar cualquier función con la precisión deseada mientras que esta posea un número finito de discontinuidades, para lo cual esta precisión depende de la selección del número correcto de neuronas en la capa oculta, en esta red la capa oculta es la capa recurrente, el retardo que tiene en la conexión de la realimentación almacena los valores de una iteración previa para utilizarlos en la siguiente iteración.

Se puede dar el caso de que dos redes de Elman tengan las mismas características, incluso en los patrones de entrada, sin embargo estas pueden entregar salidas diferentes debido a sus estados de realimentación.

La similitud de la red de Elman con la Backpropagation permite que su entrenamiento sea similar basados en técnicas de optimización del gradiente conjugado como se explicó en la red mencionada continuando con los siguientes pasos:

- Con los patrones de salida se propaga inversamente para encontrar la gradiente del error para los conjugados de pesos y ganancias.
- Se actualizan todos los pesos y ganancias con el gradiente encontrado.
- La desventaja principal de la red de Elman es que se calcula el gradiente en base a una aproximación de error, pero para esto es necesario más neuronas en la capa oculta lo que le haría más complicado el proceso de ajustar los pesos y lentitud por cada neurona. (Albanés & García, 2011)

2.6 IDS e IPS

Como se mencionó en las políticas de seguridad es necesario implementar herramientas que permitan monitorear el estado del tráfico, su funcionamiento, niveles de accesibilidad a los recursos de la red, confidencialidad y la integridad de este, de ahí que elegirlas depende de su uso y bondades que estas ofrecen, estas herramientas buscaran identificar posibles intrusiones antes de que ocurran o mientras están ejecutándose ya que los intrusos normalmente buscan adueñarse o utilizar para algún fin el sistema que atacaron, instalando software que les permita el futuro acceso, que borre sus huella mientras estuvieron presentes, keyloggers[14], software de spamming[15], virus tipo botnet[16], spyware[17], entre otros.

[14] Software o dispositivo de hardware que se encarga de registrar las pulsaciones en el teclado para luego memorizarlas en un fichero.
[15] Correo o información basura de los mensajes no solicitados, no deseados o remitente no conocido.
[16] Conjunto o red de robots informáticos que se ejecutan de forma autónoma.
[17] Malware que recopila información de un computador para luego transmitirla a una entidad externa sin el consentimiento del propietario.

2.6.1. Sistema de Detección de Intrusos (IDS)

Un IDS es una herramienta que sirve para monitorear el tráfico que fluye en una red, ubicado en un lugar estratégico, permite obtener una copia exacta de este, sin interrumpir los procesos comunes de la red, es una herramienta pasiva, quiere decir que solo detecta ataque pero no lo detiene, lo cual es considerado como una desventaja. El IDS recibe información y la cataloga como tráfico normal, anormal o maligno dependiendo de cómo se configuró al inicio, para luego disparar alertas indicando que existió una intrusión en el sistema, todo depende de cómo se implementó, las intrusiones pueden almacenarse en una base de datos como (logs[18]), pueden ser notificadas al administrador mediante correo o incluso pueden ser enviadas directamente a aplicaciones externas que ayuden a controlar dicho tráfico.

Para utilizar un IDS se considera varios factores y funciones:

- Identificar ataque y vulnerabilidades en el sistema mientras está ocurriendo o poco después.
- Identificar inicios de un ataque.
- Informar sobre el riesgo en una organización.
- Si ha existido un ataque incluso si este falla, informar cómo se ha producido o como se está produciendo este.
- Automatización de la búsqueda de nuevos patrones de ataque con herramientas estadísticas de búsqueda y análisis de anomalías en tráfico.

[18] Archivos en los cuales se registran eventos que suceden al utilizar un dispositivo o una aplicación en particular.

- Auditoría de configuraciones y vulnerabilidades en determinados sistemas.
- Varios usuarios de la red o el sistema pueden aprovechar de sus privilegios que disponen para dar mal uso a la información disponible y realizar actividades en su beneficio.
- Automatizar tareas para actualizar reglas u obtención y análisis de logs, configuraciones de firewalls entre otras aplicaciones.

2.6.2.1 Clasificación de los IDS

Existen dos tipos principales de IDS que orientan su trabajo de acuerdo a su ubicación y objetivo:

2.6.2.1.1 IDS con detección orientada a Host (HIDS)

Este tipo de Sistema de Detección de Intrusos permite monitorear el tráfico que fluye por el host en el cual reside este, obteniendo toda su información local, mediante sus procedimientos se puede saber con facilidad que usuario estuvo involucrado en un ataque, permitiendo inclusive observar si el ataque fue exitoso y efectivo o no, una gran ventaja de uso de este tipo de IDS es que se puede conocer los ataques en el origen lo que un IDS de red no permite, lo más importante es que este puede hacer un análisis de tráfico antes de que los datos sean cifrados o luego de ser descifrados, las desventajas es que son muy costosos de administrar en forma individual, si el analizador se encuentra dentro del host que se realiza el monitoreo este puede ser deshabilitado mediante los mismos atacantes al tener éxito, no permiten realizar un análisis a una red ya que solo analiza lo que le llega a su host de

residencia, y el principal problema es que reduce los recursos del host que está monitoreando limitando el rendimiento del sistema que ocupa.

2.6.2.1.2 IDS con detección orientada a Red (NIDS)

Este tipo de IDS en cambio monitorea el tráfico que fluye por la red mediante su captura y análisis, puede monitorear varios host dependiendo de la posición del sensor y su configuración le permite mantenerse en forma transparente evitando ser detectados durante un ataque, su capacidad para analizar varios host le hace una herramienta muy potente pero todo depende de la cantidad de tráfico que está monitoreando, su forma pasiva de funcionamiento evita utilizar demasiados recursos de la red evitando interferencias en la misma, también pueden ser configurados para que sea invisible a la red, lo cual lo convierte es sistemas muy seguros, de la misma manera sus desventajas radican en la cantidad de tráfico que se está capturando ya que este puede ser muy elevado en comparación a la capacidad de la CPU en la cual reside el sensor, otro problema que es solo pueden saber que un ataque fue lanzado pero no saber si este fue exitoso o no, lo cual obliga a los administradores a realizar análisis adicionales en forma manual en cada host, en algunas ocasiones se han encontrado ataques elaborados en forma fragmentada para que no parezca una intrusión o a la ves parezca una intrusión pero sin objetivo alguno provocando falsos positivos o negativos confundiendo a los administradores y muchas veces permitiendo este tráfico ingresar sin problema, los NIDS no detectan este tipo de ataques provocando inestabilidad y en varias ocasiones haciendo el sensor caiga. (Santillan, 2011)

Como se mencionó anteriormente, la ubicación del sensor IDS permitirá obtener los resultados esperados para detener el tráfico anormal o malicioso, esto se lo puede hacer contando con la ayuda de un firewall para reducir un poco el tráfico excesivo, tomando en cuenta las siguientes formas:

- Sensor antes del firewall: Se lo puede colocar fuera de la red antes de que ingrese al firewall Figura 41, de esta manera se puede capturar todo el tráfico entrante, el problema es que mucha información puede superar el CPU de la máquina donde reside el sensor y colapsarlo o generar falsas alarmas que no puedan ser controladas con facilidad por el administrador de la red.

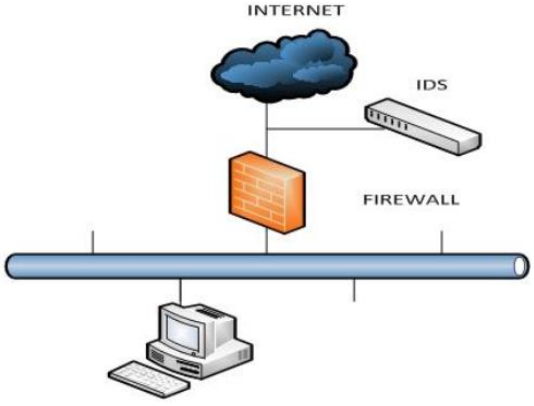


Figura 41: Sensor IDS ubicado antes de un firewall
Fuente: (Chanaluisa, Meza, & Tasipanta, 2012)

- Sensor dentro del firewall: En este caso el sensor estará ubicado dentro de la máquina que disponga de un firewall, pudiendo de esta manera ser controlado el tráfico que primero es analizado por dicho firewall para luego recibirlo el sensor, así se evita falsas alarmas, a la vez será controlado el tráfico malicioso que no es detectado y el

administrador de la misma podrá responder a tiempo en caso de un ataque, sin embargo el hecho de tener dos herramientas en una sola maquina también puede provocar colapso en la estructura de esta.

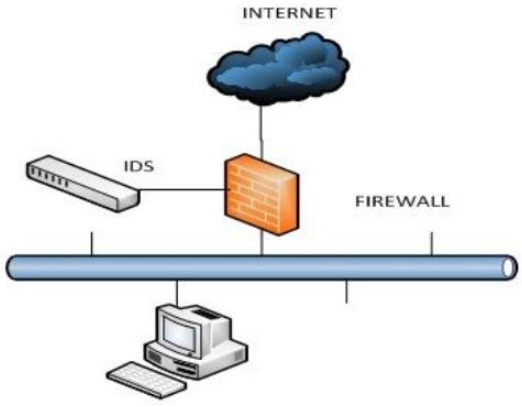


Figura 42: Sensor IDS ubicado dentro de un firewall

Fuente: (Chanaluisa, Meza, & Tasipanta, 2012)

- Sensor después del firewall: Al colocar un sensor IDS después del firewall se da la posibilidad de detectar información maliciosa que no ha sido detenida anteriormente Figura 42, esto facilita mucho para que los administradores puedan actuar rápidamente en caso de un ataque y el sensor puede administrar en su mayoría la red dependiendo como haya sido configurada, en este caso lo más aconsejable poner un NIDS a diferencia de los anteriores escenarios donde se utiliza un HIDS.

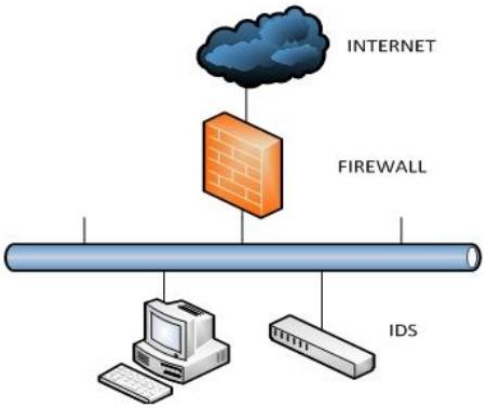


Figura 43: Sensor IDS ubicado después de un firewall

Fuente: (Chanaluisa, Meza, & Tasipanta, 2012)

La posición de un sensor IDS depende de la infraestructura que se disponga tanto en software como hardware, en algunos casos cuando los recursos son suficientes se suele colocar sensores antes y después del firewall garantizando de esta manera la detección de intrusiones y ataques Figura 43, la desventaja como se mencionó al principio es que los IDSs solo pueden detectar e informar de ataques mas no detenerlos (Astudillo, Jimenez, & Ortiz, 2011).

Un IDS es un sistema montado en un dispositivo físico o lógico que permite analizar el tráfico en la red, pudiendo proveer de información específica acerca de una actividad que se ha detectado, ya que su forma de análisis es más profunda en cada paquete a diferencia de los firewalls, todo este análisis lo basa en el tráfico capturado o anomalías en la red.

- **Detección de firmas**: Es un patrón con características conocidas de amenazas detectadas anteriormente en las cuales se incluyen: dirección del flujo, tipo de tráfico, protocolos, direcciones IP, puestos origen y destino y en muchos casos el contenido

del paquete analizado, durante este proceso cuando un paquete coincide con el patrón establecido se lanza inmediatamente una alerta de seguridad en la cual se informas la relación con el patrón preestablecido, estos patrones el administrador debe estar actualizándolos constantemente y lanzándolos a la red para que sean reconocidos.

- **Detención por anomalías**: Esta establecido en la red un cierto funcionamiento considerado normal por el administrador y las aplicaciones como bases de tráfico, cuando el sensor IDS detecta una actividad fuera de lo establecido como normal en un determinado rango es considerado una anomalía y propuesto como trafico malicioso. (Santillan, 2011)

El hecho de utilizar un IDS no quiere decir que la estructura esta lista para detectar intrusiones sin tener error alguno, hay que tomar en cuenta que se van a generar falsos positivos o falsos negativos y cuando la tasa de este tipo de errores es muy grande no sirve de mucho a aplicación de estas herramientas, para evitar estos problemas se genera la ecuación:

$$Presición = \frac{ataque\ reales\ detectados}{ataques\ reales\ detectados + falsos\ positivos}$$

Siendo la precisión el margen de error que se quiere disminuir al momento de analizar el tráfico, hay que tomar en cuenta que esta fórmula no responde a todo tipo de errores, pero como un punto de partida ayuda mucho para elaborar algoritmos de detección. (Martinez, 2011)

2.6.2. Sistema de Prevención de Intrusos (IPS)

Al igual que los IDSs, el IPS permite monitorizar el tráfico que fluye en una red buscando anomalías o comportamientos anómalos, pudiendo este ser aplicaciones software o hardware (dispositivos) orientados a ejercer el control de acceso en una red informática para proteger a los sistemas computacionales de ataques o intrusiones, a diferencia de los cortafuegos tradicionales toma decisiones basándose en lo que contiene el tráfico y no en la direcciones IP o los puertos de donde provienen, de ser necesario puede realizar cambios en el entorno de seguridad o cambios en los contenidos del ataque inclusive puede ver los ataques en los firewalls, pueden investigar el contenido y los archivos de registro de firewalls, routers, etc. El IPS a más de monitorizar el tráfico entrante en la red puede filtrar y bloquear paquetes mediante técnicas de caída de conexión, paquetes ofensivos, bloquear intrusos sin importar el protocolo de transporte que estos utilizan o reconfigurar dispositivos externos, inclusive puede bloquear a un anfitrión atacante, y este ataque incluir en una bitácora, enviando alarmas a la consola de administración.

Los procesos realizados por los IPS dependen de la configuración por parte del administrador y las necesidades del cliente, estos pueden ser 5X8 o 7X24 para agregar, editar o eliminar firmas de su respectiva base de datos, realiza análisis de logs del dispositivo que se administra y hace una correlación con logs de otros dispositivos que tenga contratados el cliente, todo esto lo realiza con reportes de servicios con frecuencia mensual y ante la ocurrencia de incidentes y eventos especiales.

Los IPS clasifican su detección de tráfico mediante las siguientes categorías:

- Basado en firmas: Al igual que los antivirus, contiene un archivo de firmas que comprende un paquete de firmas de red que son patrones de ataque que están pre-configurados y predeterminados, el cual está elaborado con la intención de servir como archivo de actualización para nuevas amenazas y comportamiento malicioso conforme se descubren las 24 horas y que son publicadas como nuevas en forma regular, para actualizar a las bases de datos de firmas que reside en algún dispositivo con funciones IPS o IDS, siendo estas firmas patrones de datos contenidos en un archivo, de esta manera el IPS realiza comparaciones entre el tráfico de red y los patrones de datos de firmas para detectar una conducta de tráfico sospechoso y luego actuar.
- Basado en políticas: De acuerdo a las políticas de seguridad que fueron declaradas por el administrador.
- Basado en anomalías: Depende del comportamiento normal o anormal del tráfico, siendo un análisis estadístico basado en el rendimiento promedio de las condiciones de tráfico de la red, creándose una línea de base para el comportamiento, luego el sistema realiza lecturas de las muestras del tráfico en forma intermitente para luego compararlas con las muestras de la línea de base, si la actividad se encuentra fuera de los parámetros de referencia base el IPS toma la acción apropiada de la configuración.
- Honey Pot: Se utiliza un equipo que funciona de distracción para los atacantes.

Los IPS son implementados en la red como agentes instalados en el sistema a proteger, monitoreando al núcleo del sistema y sus servicios, incluso interceptando llamadas al sistema o APIs[19], además se incluye que en la actualidad el IPS dispone de funcionalidades de los firewalls y antimalware[20], de igual forma dependiendo de su configuración se debe tener en cuenta que no debe interferir con los procesos de los sistemas operativos de cada host y procesos de la red mientras este actúa, esto quiere decir que debe ser estable, no debe impactar en el rendimiento del sistema, y no debe bloquear actividades legítimas.

Los IPSs pueden funcionar de acuerdo al tipo de equipo o programa a proteger estos se dividen en:

- NIDPS: monitorean el tráfico de segmentos particulares o equipos de una red, analizando protocolos de red, aplicación y transporte, buscando actividades sospechosas.
- HIDPS: monitorea tráfico que llega a un servidor o equipo final combatiendo las intrusiones una vez que se encuentra en peligro, complementando las acciones del antivirus y evitando fuga de información.
- Ambientes virtuales: Mucha información se encuentra fuera de la estructura física de la red en búsqueda fomentar el ahorro de energía, bajo costo de equipamiento y mantenimiento, reduciendo espacio físico y obteniendo mayor capacidad de

[19] Conjunto de subrutinas, funciones o procedimientos que pueden ser utilizado por cualquier programa.
[20] Programa diseñado para prevenir, detectar y remediar software malicioso en los dispositivos informáticos y sistemas.

procesamiento, aquí es donde el IPS puede actuar al momento de proteger la información inclusive actuando en la capa de aplicación inspeccionando el contenido de los datos.

- WIDPS: Estos analizan protocolos inalámbricos en búsqueda de actividad sospechosa, utilizando un solo canal por cada análisis siendo esto una desventaja, pueden ser utilizados para equipos dedicados o APs[21] con funcionalidad de IDPS. (Ware, 2011)

2.6.2.1 IPS según sus funcionalidades de código privativo y software libre

2.6.2.1.1 IPS de código privativo

El trabajo que realiza el planeta en favor del código abierto permite que muchas aplicaciones tengan la posibilidad de ser aceptadas por los usuarios, dando grandes beneficios por su rendimiento y funcionalidad, sin embargo el hecho de no tener el respaldo por organizaciones privadas provoca que este avance lentamente o no tenga el soporte informático necesario, en cambio el código privativo recibe grandes sumas de dinero en favor de dar una mejoría diaria a sus creaciones pero con altos costos en sus licencias, con la ventaja de que sus funciones son en la mayoría estables y cumplen sus objetivos con facilidad, a continuación se describe software IPS a nivel de hardware con sus características

[21] Dispositivo que conecta equipos de comunicación inalámbrica.

básicas, ventajas y desventajas descrito por el Cuadrante Mágico de Gartner[22] Figura 44, según estudios realizados en el año 2015:

Figura 44: Lideres IPSs según Gartner Agosto – Noviembre 2015

Fuente: (Carlson, 2015)

[22] Análisis de tecnología que realiza la consultora Gartner mediante cuadrantes y los ciclos de sobre expectación, proporcionando consejo relacionado con la industria/sector y el apoyo al gobierno para los profesionales de las TICs.

Tabla 1: Características de dispositivos IPS líderes en el año 2015 (Elaborado por autor)

FABRICANTE	DESCRIPCION	VENTAJAS	DESVENTAJAS
IBM (XGS)	- Alta calidad de firma y baja latencia, espectro de soluciones que pueden llegar a 8Gbps con un dispositivo y 40Gbps con sistemas de tarjeta blade. - Tasas de transferencia hasta 8Gbps. -Tecnología FlowSmart con inspección inteligente. - Reputación de abordo / IP y control de aplicaciones.	- Interfaz entre IBM y clientes – socios. - Actualización constante desde sede de operaciones. - Alta fiabilidad. - Fácil implementación, - Gestión de seguridad centralizada. - Soporte a problemas	Problemas de comunicación entre los sensores de Network IPS y el SiteProtector Management software
Check Point	- Otorga geo – protección.	- Seguridad de última generación.	- Vulnerabilidad en ataques DDoS basados en el

	- Monitoreo en tiempo real. - Multi gigabit y gestión de amenazas dinámico. - Gestión unificada. - Despliegue sin dolor - Inspección SSL	- Multigigabit de rendimiento. - Menor TCO[23] y mayor ROI[24].	rendimiento de la puerta de enlace.
Sophos	- Protección multiplataforma desde una sola consola. - Utiliza tecnología de borrado remoto y antirrobo. - Las implementaciones funcionan en forma local o en la nube en forma integral.	- Bajo consumo de recursos. - Fácil implementación. - Acepta varios dispositivos sin aumentar costes. - Escanea el contenido de los datos en tiempo real antes de que llegue al navegador.	- Falsos positivos que impiden descargas confiables. - Con una configuración errónea hay que parar el IPS para corregirlo, durante ese tiempo queda la red totalmente vulnerable.

[23] Costo total de proveer y mantener una solución informática.
[24] Beneficio que se obtiene por cada unidad monetaria invertida durante un período de tiempo.

	- Utiliza DLP[25] y cifrado de correo electrónico. - Implementa cifrado de discos completo.		
Cisco	- Capacidad máxima de procesamiento de inspección 10Gbps. - Conexiones máximas 8400000. - Latencia media menos de 150. - Correlación Global. - Selección de mitigación basada en la reputación. - Análisis compuesto de firmas. - Calificaciones de firmas - personalizable.	- Protección específica para Data Center en servidores basados en la Web, bases de datos y almacenamiento. - Defensa a los servidores más fundamentales. Fácil implementación y gestión.	- Desconexiones del IPS hacia la red por falta de certificados. - Sensores desconectados cuando se actualiza a una nueva versión. - Las firmas no se actualizan automáticamente dentro de los periodos de gracia. - Números grandes de pedidos de RADIUS.

[25] Prevención de pérdida de datos para evitar que los usurarios envíen información sensible fuera de la red.

McAfee	- Tecnología en capas sin firmas. - Análisis de archivos en profundidad con inspección en JavaScript basada en protocolos. - Utiliza correlación en tiempo real de los eventos de red. - Rendimiento y escalabilidad. - Un solo motor de análisis que integra varias funciones mediante emulación. - Prevención ante ataque DoS y DDoS, basado en umbrales y análisis heurístico. - VPN de protocolos.	- Respuestas rápidas ante amenazas. - Alto rendimiento de la red sin importar la situación de inspección de ataques. - Prioriza los dispositivos que están siendo atacados. - Alta disponibilidad. - Autenticación de usuarios (RADIUS y LDAP). - Protección frente a redes de bots. - Administración centralizada.	- Sin errores críticos conocidos o documentados. - Incompatibilidad entre host IPS 8.0 y MA 5.0.

Fortinet	- Gestión a base de una sola consola. - Protección avanzada contra amenazas. - Conmutación integrada. - Aplicación de políticas de punto final. - Interfaces de alta velocidad de hasta 10 GbE con alta densidad de puertos. - Balanceo de carga. - Aplicación de QoS en los dispositivos. - Control de redes inalámbricas extendidas. - VPN	- Gran rendimiento con baja latencia. - Sistema operativo de seguridad FortiOS avanzado y flexible. - Actualización en tiempo real. - Aumento de visibilidad de la red.	- Fallas de certificados al realizar las actualizaciones del firmware y los navegadores.

Al igual que el alto rendimiento disponible en dispositivos IPS privativos, también se encuentra software IPS libre para empresas con poco presupuesto que buscan controlar intrusos dentro de sus redes, a continuación se describen las características de los IPSs más comunes:

Tabla 2: Características de los principales IPS Software Libre (elaborado por autor)

FABRICANTE	DESCRIPCIÓN	VENTAJAS	DESVENTAJAS
SNORT	- Soporte de múltiples hilos de procesamiento de paquetes. - Configuración y tabla de atributos compartida. - Componentes clave enchufables. - Tampones pegajosos en reglas. - Posee más de 700 firmas.	- Fácil implementación. - Soporte multiplataforma. - Se apoya en BASE[26] IPS. - Se consolida como motor de EASYIDS. -Con la ayuda de herramientas adicionales se puede administrar múltiples sensores en la red.	- En líneas de tráfico por donde fluyen datos a altas velocidades se imposibilita analizar todo permitiendo anomalías con facilidad o produciendo falsa alarmas. - IPS Snort aún se encuentra en

[26] Software de análisis de seguridad basado en Snort.

	- Es de distribución gratuita.		desarrollo para constituirse en sí. - Es mono proceso, no pudiendo aprovechar los núcleos multi-core. Incapacidad de reconstruir lo que está ocurriendo en un sistema que está siendo monitorizado.
SURICATA	- Arquitectura multi – hilos. - Estadísticas de rendimiento. - Detección de protocolos automáticos. - Reputación IP.	- Ideal para Pymes[27]. - Arquitectura multiproceso lo que le permite aprovechar las bondades de los núcleo core.	- Througput limitado dependiendo del tráfico en la red. - No realiza actualizaciones en tiempo real, tiene que reiniciarse en cada sesión.

[27] Pequeñas y medianas empresas en las cuales se implementa tecnología y soluciones informáticas.

	- Aceleración con GPU.	- El desarrollo de sus procesos está en evolución. - Se consolida como motor de SMOOTHSEC.	- Falta de integración de motores para detección.
SAMHAIN	- La detección y prevención de intrusos lo realiza a nivel de Host. - Realiza monitoreos íntegros de archivos en los Host. - Interfaz web. - Actualización de la base de datos de firmas centralizada. -Supervisión de puertos.	- Las anomalías son reportadas inmediatamente. - Ofrece líneas base de los sistemas operativos lo cual ayuda en el ahorro de tiempo con la detección. - Es invisible en la lista de procesos del sistema operativo. - Puede controlar múltiples host con diferentes sistemas operativos.	- Instalación y configuración poco amigable con el administrador.

CAPÍTULO 3

ANALISIS DE TECNOLOGIAS

3.1 JUSTIFICACIÓN DE TECNOLOGÍAS DE REDES NEURONALES ARTIFICIALES A UTILIZAR.

Las redes neuronales están caracterizadas de acuerdo al tipo de datos que pueden analizar y filtrar, la menor tasa de errores que cometen; lo que permite resaltar la utilización de la red en la tarea asignada, sus ventajas y desventajas, y justificar cual es la mejor opción para ser utilizada en el trabajo propuesto, como por ejemplo:

La red PERCEPTRON de una sola capa que se creó inicialmente, está compuesta por la función de transferencia Hard Limit, sus entradas son vectores patrones bidimensionales expresadas como coordenadas que puedan ser divisibles en el plano como variables, ejemplo: datos expuestos de la velocidad en los cuales interviene el desplazamiento y el tiempo que pueden ser representados en los ejes (x, y), esperando localizar los datos (puntos) que se encuentren cerca del origen como promedios de solución de esta red, siendo los pesos w la frontera de decisión en la cual se encuentra la recta que va a dividir a los valores deseados obteniendo los resultados sobre la recta o bajo esta, a los cuales se les puede asignar 0 y 1 respectivamente como las salidas, la ecuación de esta red es $a_i = hardlim\ (Wp + b)$, mediante la cual el aprendizaje puede ser generalizado, lo que le permite aprender nuevos patrones a partir de los ya conocidos.

Como desventaja de la utilización de esta red tenemos que solo sirve para clasificar problemas linealmente separables y solo se puede saber si hubo equivocación o no, lo cual

ya han sido estudiados con métodos estadísticos de mayor eficiencia. (Andrade, PRINCIPALES DE REDES NEURONALES, 2013)

La red ADALINE está dada en base a características del Perceptrón con la diferencia de que esta tiene salidas lineales y con valores reales y se puede saber cuánto de error existe, su salida neta (suma ponderada de entradas) es igual a su función de activación, toma valores continuos desde negativos hasta positivos, su regla de aprendizaje es el mínimo cuadrado (LMS), mediante métodos de optimización de errores llamado gradiente descendiente lo cual le da su característica principal ya que este algoritmo le permite reducir los errores mediante iteraciones y encontrar su máximo incremento o su mínimo, en este caso se supone que es el mínimo valor que se desea encontrar, el LMS busca minimizar el error de la salida de la neurona (diferencia entre el valor deseado y el valor actual).

La desventaja principal de esta red es que el hecho de ser una red supervisada se debe poner valores a la constante de error, al ser reducida por la gradiente y tomar valores para la constante hay que tener claro que no se le puede poner valores muy altos porque se creara una sobre corrección y no llegará la mínimo deseado, y si el valor de la constante es muy pequeño le tomará mucho tiempo en encontrar dicho error, en consecuencia solo resuelve adecuadamente problemas binarios linealmente separables, la ecuación de la red ADALINE queda expresada:

$$a = purelin(Wp + b)$$

En algunos casos para resolver problemas en las redes es necesario poner más de una neurona con capas de salida y capas ocultas las cuales permitirán resolver problemas que no

son linealmente separables, la red ADALINE o PERCEPTRON si permite el funcionamiento con varias capas, sin embargo el hecho de que son redes supervisadas al momento de extrapolar las salidas con las entradas si no fueron correctamente entrenadas se puede obtener salidas imprecisas las cuales deben modificarse a través de su peso en forma manual, otro problema son los mínimos locales, una vez alcanzados no se puede continuar entrenando así no se haya obtenido una convergencia ideal, es aquí donde la red BACKPROPAGATION (siendo la unión de varios perceptrones y utilizando procesos de Adaline) actúa al momento de obtener las salidas, estas son restadas con las salidas deseadas y multiplicadas por la derivada de la función de transferencia sigmoidea en cada nodo.

Una vez obtenidos los errores en cada nodo comienza la retro propagación con la intención de modificar los pesos, en este momento se encuentran los errores en las capas ocultas retro propagándose hacia la capa de entrada y modificando los pesos en cada iteración utilizando la fórmula:

$$\Delta W(t+1) = W(t) + \alpha \varepsilon x$$

Cada uno de los errores de los nodos de las capas ocultas se puede calcular mediante la fórmula:

$$\varepsilon_{no} = (\sum_{na}^{n} \varepsilon w)(1 - Y_{na})Y_{na}$$

Siendo:

ε_{no} el error obtenido en las salidas de la red.

($\sum_{na}^{n} \varepsilon w$)la sumatoria de los errores de los nodos que están conectados al nodo de la capa oculta.

$(1 - Y_{na})Y_{na}$la derivada de la función de transferencia que se obtuvo de derivar la salida de cada nodo $Y_{na} = \frac{1}{1+e^{-Neti}}$.

$Neti = \sum_{i=1}^{n} X_i W_i$ es la sumatoria de las entradas de cada nodo por sus pesos conectados a los nodos de la siguiente capa de la cual es calculada su Neti.

Una de las desventajas principales de la red Backpropagation es que no se puede definir los errores de nodos de las capas ocultas, lo que conlleva que demorar el ajuste de los pesos al caer en el error de los mínimos locales, otro caso es que si se pone valores muy altos o muy bajos el aprendizaje si se logra, pero provocando lentitud con lo que se definiría una parálisis en el proceso, en el aprendizaje lo recomendado es -5 a 5 y por último si no se llegara a encontrar los pesos adecuados la iteración se hace infinita, tomando en cuenta estas características se puede concluir que en la red backpropagation no es posible predecir el tiempo de convergencia, esto quiere decir que al tener grandes volúmenes de información provocaría un proceso muy alto con lo cual no es ideal en el caso de querer analizar tráfico en una red.

Con lo mencionado anteriormente Hebb propone una red con características de relación entre las entradas y salidas a lo cual las llama redes ASOCIATIVAS con la intención de que estas redes reduzcan el tiempo de convergencia al ajuste de los pesos y procura evitar los mínimos locales al fortalecer la sinapsis (aprendizaje), por ejemplo si durante un aprendizaje una entrada p_i tiene un valor positivo y una salida a_j también tiene un valor positivo su

función se activara y su peso será proporcional al producto de sus funciones de activación en cualquier lado de la sinapsis y el peso entre ellas se incrementa, determinando el incremento por:

$$w_{ij}^{nuevo} = w_{ij}^{anterior} + \alpha(a_{iq})(p_{jp})$$

A partir de este tipo de redes Grossberg propone realizar una relación entre la diferencia de las entradas y sus pesos al experimentar las iteraciones a las cuales las llama INSTAR con características del Perceptrón, procurando que esta diferencia iguale las entradas con los pesos, al tener esta igualdad se dispararía el umbral de la neurona y su función provoca salidas 1 en caso contrario al ser diferentes se provoca una salida 0, de igual manera se complementa las salidas deseadas, siendo estas un patrón de relación con los pesos obtenidos, esto quiere decir que se busca modificar los pesos para obtener una salida específica buscando la diferencia entre las salidas de las neuronas y sus pesos, a esta se la llama OUTSTAR, entonces al combinar INSTAR y OUTSTAR se puede reconocer patrones y generar configuraciones que se desean.

En las redes asociativas su desventaja principal es que no tiene un mecanismo específico para decrementar pesos o hacerlos estables conllevando a que estos crezcan infinitamente, quiere decir que para cada asociación toca aumentar reglas de degradación pero con estímulos repetidos o se pierde la asociación, en análisis de tráfico abundante esto provocaría procesos adicionales con lo cual aumentaría costos en recursos.

Categorizando tipos de aprendizajes de las ANN nos encontramos con otra forma de receptar información y excitar a una neurona, al obtener entradas se conoce que las neuronas

en el cerebro pueden competir unas con otras para lograr una tarea obteniendo una ganadora que puede autoexcitarse a la cual se la llama positiva y las que no pueden hacerlo están inhibidas o son negativas a las que se las llama vecinas, de esta manera se puede clasificar información similar entre las neuronas categorizando los datos de entrada en la red y provocando que se active la neurona de salida, de esto parten las redes Competitivas las cuales utilizan inhibición lateral. Una vez clasificadas las entradas donde las neuronas que se encuentran cercanas a un vecindario de la neurona ganadora respondan a entradas similares, estas pueden ser organizadas utilizando redes multicapa las cuales pueden dividir cada capa en grupos de neuronas que disponen de conexiones inhibitorias con otras neuronas del mismo grupo o excitatorias con las demás capas, tomando en cuenta que estas pueden tener inhibición mutua cuando están a cierta distancia unas con otras con respecto a los valores de sus pesos.

Aquí es donde la red de Kohonen presenta un sistema de organización de zonas con la información recibida representándolas en mapas bidimensionales formando de esta manera mapas topológicos siendo de tipo off – line donde se puede distinguir las capas de aprendizaje con las de funcionamiento, en la primera se fijan valores de conexiones entre las capas de entrada y salida en las cuales en la salida compiten por su activación y solo una permanece activa, repitiéndose el proceso hasta obtener los resultados requeridos por el mapa topológico de salida, reduciendo con esto la zona de neuronas que se deben activar, a diferencia de la red INSTAR, KOHONEN activa sus neuronas ganadoras en base a una entrada con características similares en base a un mapa organizado por un vecindario.

Otra de las redes competitivas existentes es la red de HAMMING con una estructura más compleja ya que tiene una segunda capa en la cual utiliza redes recurrentes, de igual forma que KOHONEN sus salidas compiten por obtener neuronas ganadoras las cuales representan el patrón prototipo más representativo a las entradas, esta red utiliza dos capas, la primera una red instar la cual hace una correlación entre las entradas y los patrones prototipos y la segunda realiza la competición para saber cuál de estos patrones prototipos es el que está más cercano a la entrada, en la salida solo una tendrá una salida no cero la cual se encuentra categorizada en un grupo que se relaciona con la entrada, en esta red cada neurona se excita a si misma e inhibe a todas las otras neuronas, su función será:

$$a = compet(n)$$

Esta reemplaza a la capa recurrente, y para que se pueda realizar varias tareas se tiene que utilizar varias INSTAR ya sea en la capa de aprendizaje o en la 2da capa lo cual le representa una gran desventaja al momento de crear una red competitiva ya que KOHONEN y HAMMING permiten clasificar patrones en base a características similares pero cuando se tiene tráfico en una red con infinitos estados se tendría que utilizar muchas INSTAR o capas recurrentes a lo cual los procesos necesitan hardware muy robusto y con características de crecimiento. Otra desventaja es que el vector de pesos inicial de una neurona se encuentra muy lejos de cualquiera de los vectores de entrada, por lo cual puede darse el caso de que nunca gane la competición y se convierta en una neurona muerta.

Cuando una red tiene una topología cíclica se la denomina red recurrente teniendo estos un profundo impacto en la capacidad de aprendizaje especialmente para el procesamiento de

secuencias temporales lo cual le diferencia mucho con las ANN mencionadas anteriormente ya que estas redes tienen capacidad de tener conexiones consigo misma esto quiere decir que pueden autoestimarse y modificar su propio peso, conexiones entre neuronas de una misma capa lo cual le permite excitar a otra neurona y está a la ves a la primera, conexiones entre neuronas de una capa anterior lo que si encuentra un error al propagar una entrada en la siguiente neurona esta puede volver a reajustar sus pesos en función de la anterior. En las redes recurrentes se utiliza probabilidades para localizar características específicas en las entradas lo que permite tener una ventaja sobre el tráfico malicioso ya que este ingresa con cambios de sus datos, información y estructuras y esto dificulta la inspección para un antivirus común o para un IDS/IPS. Las redes recurrentes pueden predecir secuencias, frases, audio, curvas de luz, entre otras, se puede decir que son redes completas ya que inclusive pueden fusionarse con las redes BACKPROPAGATION, sin embargo un problema de estas recurrencias está en el momento de la iteración para derivar una capa oculta respecto a un peso lejano intentando reducir su gradiente entre estas, a lo cual al multiplicar N veces su vector de pesos tiende al infinito o a cero respectivamente lo mismo que se le conoce como memoria inestable o limitada, a la primera se la puede corregir con facilidad proporcionándole un limitador simple cuando su gradiente este incrementándose mucho, pero para la segunda cuando la gradiente se tiende cero no se pude poner un limitador, no

obstante se creó la estructura LSTM[28](Long Short-Term Memory) con su memoria a corto y largo plazo utilizando el descenso de su gradiente $\varepsilon(t) = \frac{1}{2}\sum_{i=1}^{n}(d_i[t] - y_i[t])^2$.

Existen un sinnúmero de aplicaciones de las redes RECURRENTES entre estos y los que sigue este trabajo es el reconocimiento de cadenas de caracteres en estado binario y hexadecimal en un canal de tráfico que pudo haber sido intervenido por un tercero para adecuar patrones que sigan un determinado proceso a conveniencia afectando la información en diferentes estados, las redes recurrentes tienen la capacidad de analizar un lenguaje y corregirlo para que este esté correctamente escrito, puede controlar sistemas reales de manera que sus salidas sigan un determinado patrón temporal o dinámico gracias a su variable tiempo lo que le permite ser adecuado para manejar altas tasas de tráfico en un canal sin necesidad de acudir a hardware muy sofisticado. En las redes neuronales recurrentes también se puede hacer uso de entrenamiento con supervisión en línea y en tiempo real y como se mencionó anteriormente con memoria a corto y largo plazo lo que le permite reconocer patrones con características específicas en las entradas.

Una de las redes principales entre las recurrentes es la HOPFIELD, red recurrente que tiene conexiones en todas las direcciones, está dada por una estado inicial de acuerdo a un patrón de entrada y un estado estable por un patrón de salida

Los patrones de aprendizaje están dados desde la entrada, y los pesos se inicializan de acuerdo a los patrones de aprendizaje, por ejemplo 50 patrones de aprendizaje, matriz de

[28] Bloque de memoria que contiene una o más celdas de memoria utilizadas en la red de Hopfield.

pesos 50 x 50, la matriz de pesos se calcula en base a 2 ecuaciones; la primera W=$\sum_{i=1}^{n}[E_i E_i^T - I]$ siendo E el vector de entrada, E^T el vector de entrada transpuesto e I una matriz identidad, la segunda $W_{ij} = \begin{cases} \sum_{k=1}^{M} e_i^k e_j^k & i \neq j \\ 0 & i = j \end{cases}$ siendo e^k cada uno de los elementos de los vectores de aprendizaje y k el número de vectores propuestos, habiendo realizado este proceso no es necesario iteraciones ya que la red aprende en la primera vez que se ajustan los pesos, solo se haría iteraciones para el funcionamiento en los cuales se compara los vectores de entrada con los patrones aprendidos clasificando las entradas de acuerdo al patrón aprendido al cual pertenece buscando similitudes entre estos, durante el funcionamiento, si realiza iteraciones, pero para comparar los vectores de entrada con los patrones de funcionamiento y clasificarlos de acuerdo al que pertenezca utilizando las siguientes condiciones; es 1 si $Si = \sum_{j=1}^{N} w_{ij} S_j > 0$, es -1 si $Si = \sum_{j=1}^{N} w_{ij} S_j < 0$, o valdrá el mismo valor si $Si = \sum_{j=1}^{N} w_{ij} S_j = 0$, esto se lo hace mediante la generación de un nuevo vector S_i que permitirá la comparación del vector generado con la fórmula presentada y el vector S_i creado anteriormente para luego comparar con los vectores de aprendizaje y localizar el patrón al que pertenece esa entrada con mayor facilidad.

El problema de Hopfield es que es de naturaleza estática lo cual provoca que si en el patrón de aprendizaje existen ciertos patrones la red comparará con esos y dará sus salidas en base a lo encontrado, si se desea obtener valores intermedio no los acepta y continua extrayendo los que aprendido inicialmente, un ejemplo es: si en el patrón de aprendizaje tiene categorías de autos como deportivo, de lujo, familiares etc., y en una entrada encuentra

un tipo de auto que tiene características entre deportivo y familiar simplemente lo coloca o familiar o deportivo pero no tiene la capacidad de aprender nuevas salidas (mínimos locales) lo cual dificulta en el momento de aprender nuevos parámetros en la red, esto lo puede hacer la red Backpropagation en este caso una recomendación es hace a combinación de estas dos redes.

En algunas investigaciones se han propuesto la utilización de Perceptrón multicapa con reducción de características, sin embargo se sabe que los ataques cada día tienen diseños más sofisticados en los que solamente ubicar características básicas de una anomalía no es suficiente ya que las mismas pueden tener estructuras metamórficas las cuales no pueden ser reconocidas fácilmente por un Perceptrón sin embargo también se propone adicionar redes Backpropagation, competitivas o asociativas pero de igual manera si no se dispone de una clasificación de patrones por características básicas y aprendizaje en tiempo real reduciendo cada vez más sus errores, se tendría que adicionar muchas capas en estas redes, lo cual provocaría el disparo de su gradiente respecto a sus pesos alejados y lo que provocaría es un LMS (Error cuadrático medio) oscilante, o lo más óptimo para una ANN dejar morir neuronas alejadas.

Por otro lado hay que tomar en cuenta que el tráfico en la red de la institución estudiada es moderado de acuerdo con los esquemas presentados, sin embargo las aplicaciones utilizadas en educación y redes sociales provocan abultamiento de dicha información, hay que ser claro que no se está utilizando comunicación por video conferencia o VoIP, pero no deja de ser una red con altas tasas de tráfico por lo tanto aplicar una ANN con reconocimiento

a problemas linealmente separables es imposible para filtrar el tráfico disponible, además de acuerdo al análisis que se propuso por Wireshark si existen vulnerabilidades medias en esta red y si se implementa una ANN asociativa se tendrá el gran problema de filtrar información procurando reducir errores, lo más adecuado sería una red SOM pero está a la ves al momento de etiquetar clústers para diferenciar el tráfico limpio del malicioso no tiene una reducción de errores óptima ya que muchas veces el código malicioso llega oculto o cifrado, para esto se tendría a adoptar una red adicional.

Debido a las razones antes mencionadas en las redes recurrentes se toma como la red más recomendable a Hopfield ya que se puede utilizar la minimización cuadrática que no necesita ser entrenada con anterioridad ni realiza procesos de aprendizajes básicos sin embargo si es posible determinar pesos, ya que se puede alcanzar estabilidad y sin importar los patrones de datos ingresados sean incompletos basándose en la recuperación de contenidos almacenados se podría detener el tráfico malicioso gracias a patrones direccionales que luego de asociar los patrones almacenados con mínimas similitudes estos convergerán hacia los patrones prototipo que serán los guías para la clasificación, sin embargo hay que tomar en cuenta que también tiene inconvenientes de mínimos locales pero en esta tesis se propone especificar los patrones de aprendizaje basados en características de ataques actuales procurando destacar los más peligrosos.

En determinadas circunstancias se podría proponer la utilización de una red Backpropagation para nuevos aprendizajes y Hopfield para clasificación creando una red híbrida como es el caso de la red de Elman sin embargo hay que tomar en cuenta el tiempo

de aprendizaje que tendría esta red y su oscilación en el LMS complicaría su aprendizaje puesto que tampoco es posible calcular el número de capas de la red.

3.2 JUSTIFICACIÓN DE TECNOLOGÍAS DE SISTEMAS DE PREVENCIÓN DE INTRUSOS A UTILIZAR.

Existe en el mercado cantidades considerables de IDS/IPS que tienen la posibilidad analizar grandes volúmenes de tráfico, el problema es que involucra altos costos, tomando en cuenta que a pesar de esto si llegan a tener desventajas significativas al momento de utilizarlos, los usuarios no tienen la posibilidad de realizar mejoras, al contrario tendrán que esperar actualizaciones del fabricante lo cual conlleva a consecuencias desastrosas puesto que se conoce que han existido ataques sofisticados, en periodos de tiempo muy pequeños y en entidades prestigiosas, con software de su autoría y con alto rango en detección de ataques, caso más significativo Pentágono en EE.UU.[29], año 2008.

Por otro lado, se dispone IPSs software libre los cuales deben reunir condiciones para que sean considerados aptos en un entorno de comunicación con tráfico de cantidades voluminosas, estos deben ser: código abierto que tenga la posibilidad de permitir cambios por parte del administrador de la red mediante los cuales se creen políticas de seguridad y reconocimiento de anomalías adecuándolas a las necesidades del administrador, que disponga de una base de datos con reglas predefinidas que puedan ser ajustadas a la red que está monitorizando, que permita crear nuevas reglas, adicionar módulos extra que no sean

[29] Estados Unidos de America

parte propia de la aplicación sino que puedan ser nuevas mejoras a partir de experiencias de administradores y desarrolladores creando un potencial en algoritmos y estructuras con técnicas actualizadas y a la ves permita administrar sensores remotos con las mismas características que el original, que tenga la capacidad de monitorizar el tráfico dentro o fuera de la red o en el mismo punto del firewall, incluso al ser configurado tenga la capacidad de aplicar reglas de un cortafuegos al bloquear entrada de tráfico, que los sensores puedan ser aplicados para monitorizar tráfico de toda la red o de un Host, si se lo hace a la red lo recomendado es utilizar PCA(análisis de componentes principales) o Bloomfilter ya que la gran cantidad de datos que circula provocaría el colapso del IPS o a la ves incurre en gastos adicionales de infraestructuras nuevas, de igual manera como se mencionó que pueda monitorear la presencia de usuarios con altos privilegios en la red abusando de estos.

Por ejemplo BASE (Basic Analysis and Security Engine) tiene la capacidad de basarse en el código de la consola de analizar las bases de datos el proyecto denominado ACID proporcionando un front – end web, pero consulta y analiza alertas que proceden de Snort por lo tanto viene a ser un complemento de este, en el caso de Suricata su Througput limitado dependiendo del tráfico en la red en el caso de volúmenes grandes de datos seria inconsistente e inestable, al no ser sus actualizaciones en tiempo real provoca bugs[30] de tiempos, los cuales pueden ser aprovechados durante un ataque y su escaso grupo de motores de detección lo hacen poco aconsejable para implementación.

[30] Errores localizados en Software.

Otro caso de un IPS medianamente completo y con características software libre es Samhain el cual trabaja a nivel de host lo que también le convierte en una herramienta inusual ya que solo verificar el tráfico en un host resulta una red vulnerable a ataques y si se desea ubicar IPS en cada host impactaría en el rendimiento de la red, a más que para realizar su instalación se necesita de personal experto ya que su entorno es poco amigable, de los IPSs mencionados son los que tienen más utilización en las empresas y con mayor soporte técnico. Un último IPS que hay que mencionar es el SNORT el cual reúne características mencionadas anteriormente, a más de ellas tiene la capacidad de reconocer ataques mediante Tunelling ataques internos de la red como externos que suelen incluso aprovechar las vulnerabilidades de las aplicaciones, puede manejar sistemas híbridos, quiere decir que se puede basar en HIPS e NIPS clasificando usos inapropiados con anomalías, en los cuales al manejar HIPS se convierten en sistemas livianos y fáciles de implementar siendo indetectables teóricamente, soporta diversas plataformas, en muchos casos ha sido considerado técnicamente superior a los IPS comerciales, dispone de una bitácora de paquetes lo cual le permite reaccionar en caso de que un monitoreo de servicios sea considerado como intruso, por último se menciona que utiliza un motor de detección basado en reglas configurables lo que lo hace ideal para complementarse con una red neuronal al permitir crear nuevos módulos a más de los que contiene.

Por el hecho de disponer de ANN que crean patrones de reconocimiento de actividades no permitidas este IPS tiene la capacidad de comparar el tráfico con patrones de ataques existentes en su base de datos, la capacidad de analizar campos de los paquetes e iteraciones

en determinadas acciones y resultados arrojados por parte de los protocolos para establecer la comunicación, la similitud de sus instrucciones a lenguajes de programación C y Java y reforzar acciones con sus preprocesadores ante ataques en los cuales se pueden adicionar ANN con características de reconocimiento de anomalías fuera de las ya conocidas por los antivirus y firewalls, da la posibilidad de considerarlo el más recomendable para este proyecto al IDS/IPS SNORT.

Tomando en cuenta que las entidades de gobierno no tienen la capacidad financiera y no se permite las configuraciones de aplicaciones de seguridad directamente en caso de obtener un IPS privativo, SNORT es un IPS adecuado para utilizar en la Unidad Educativa Brethren.

3.3 TIPOS DE SENSORES A UTILIZARSE.

Como ya se mencionó con Snort puede utilizar sensores remotos mediante herramientas configurables dentro o fuera de la red, sin embargo hay que tener en cuenta que de la misma manera que el administrador puede ver el código de Snort, el atacante también lo puede hacer sin mayor problema, debido a esto el uso de sensores con mayor o menor sensibilidad en cada distribución de subredes hacia las zonas desmilitarizadas de los grados con Tablets, por otro lado mayor sensibilidad en los departamentos que disponen de información crítica para la institución poniendo en su distribución de subredes, debido a esto se opta en un inicio pruebas sin sensores excepto entre el router principal y las subredes en los cuales se utilizará como sensores la configuración de los preprocesadores stream5 y sfPortscan mediante los

cuales se pretende ensamblar el tráfico fragmentado y contar las conexiones especialmente hacia la puerta de enlace.

Hay que tomar en cuenta que como se va a utilizar características del tráfico TCP/IP para realizar pruebas es conveniente en un inicio implementar sensores NIPS buscando evitar la utilización de PCA ya que se tendría que adicionar módulos para analizar los componentes principales, sin embargo posteriormente si se tiene éxito con la clasificación de los patrones de la ANN, los sensores se implementarían en determinadas subredes para realizar pruebas con tráfico de mayor volumen de los cuales los patrones de aprendizaje de las ANN considerados con características adecuadas pueden lograr que las amenazas recaigan en ataques conocidos en los cuales estos sensores serían de gran ayuda sin embargo si se cae en los mínimos locales debido a tráfico con nuevas características, la utilización de las PCA en cada uno de los sensores será inevitable.

3.4 SITUACIÓN ACTUAL DE INFRAESTRUCTURA INFORMÁTICA EN LA UNIDAD EDUCATIVA BRETHREN (INFORME).

3.4.1 Antecedentes de la Unidad Educativa Brethren

La institución está orientada a la educación de nivel secundario con 2014 estudiantes y 85 docentes, su funcionamiento lo hace desde el año 1996 como Escuela Fiscal Brethren, hasta la fecha en la cual se ha constituido como una Unidad Educativa incrementándose su infraestructura, ciclos de enseñanza y necesidades.

3.4.2 Descripción de la red de la Institución.

La Unidad Educativa Brethren se encuentra ubicada en el sector de Llano Grande al nor-oriente de la ciudad de Quito, se encuentra distribuida por las oficinas centrales del Rectorado, Vicerrectorado diferentes departamentos y oficinas como muestra la Figura 45, hay que tomar en cuenta que se está describiendo el diseño actual de la infraestructura y el posterior diseño de la red incluyendo las zonas ubicadas con APs y la planificación de las direcciones IP que los técnicos de la institución han elaborado y los cuales rigen dentro del establecimiento para el funcionamiento de la red cableada e inalámbrica, la cual en posterior será propuesta de acuerdo a la implementación del IPS empleando ANN.

Figura 45: Infraestructura de la Unidad Educativa Brethren
Fuente: Diseño Administrador institucional

La red cuenta con una infraestructura tecnológica regular sin condiciones de cableado estructurado excepto la sección del gabinete donde reposa el router, en la cual se dispone de un laboratorio de informática que esta alimentado con una señal de internet por fibra óptica proporcionado por CNT EP, un Multiplexor tranceiver BVT BD-OP-4E1-4ETH, un router CISCO C881 con firewall incluido que se conecta a 2 APs CN40 GLY0K3 y un Switch D-Link DES-1024A para derivación a las PCs de laboratorio y tablets educativas, 6 subredes con sus respectivos Switchs genéricos y APs, 30 PCs en el laboratorio, 1 PC en secretaria, 1 PC en el DECE, 80 portátiles HP que se conectan a la red a través del AP de sala de maestros y la red LABORATORIO 2-3 Figura 46, adicionalmente se pueden hacer conexiones con sus dispositivos móviles para la comunicación y transferencia de archivos mediante de redes sociales solo para comunicación a nivel de noticias impartidas por parte de las autoridades aplicación WhatsApp, LINE y servicios de correo comerciales, todos los dispositivos se conectan mediante direcciones físicas excepto la sala de maestros que se conecta con contraseña, se da servicio de comunicación para los señores estudiantes para descargas de programas educativos para las materias impartidas tomando en cuenta que el alcance de esta red es de 10 metros orientado solo desde el AP con el nombre LABORATORIO_2 y lo pueden hacer uso durante el recreo, adicionalmente se tienen un sistema de seguridad de video que se encuentra conectados en forma aislado para monitoreo de cámaras cuando se termina las horas laborables pero son sistemas privativos que no permiten el monitoreo de tráfico y que solo disponen de acceso a las autoridades, las direcciones IP están distribuidas

en forma estática para los departamentos principales y el uso de DHCP para las subredes que hacen uso de los APs de acuerdo a la siguiente Tabla 3.

Tabla 3: Distribución de las direcciones IP para los nodos de la institución (diseño administrador red)

BRETHREN	IP pública 10.187.186.1	
DEPARTAMENTO	**IP RED**	**IP SUBRED**
Rectorado	10.187.18614	
Secretaria	10.187.186.13	
DECE	10.187.186.39	
Sala de Profesores	10.187.186.15	192.168.1.1 – 50
AP1 Laboratorio	10.187.186.11	
AP2 Laboratorio	10.187.186.10	192.168.5.1 – 50
AP3 Laboratorio	10.187.186.12	192.168.0.1- 50
AP4 Laboratorio		192.168.2.1
AP5 Laboratorio		192.168.3.1
AP6 Laboratorio		192.168.4.1
AP7 Laboratorio		192.168.5.1
AP8 Laboratorio		192.168.6.1

3.5 LEVANTAMIENTO DE DISEÑO DE RED ACTUAL

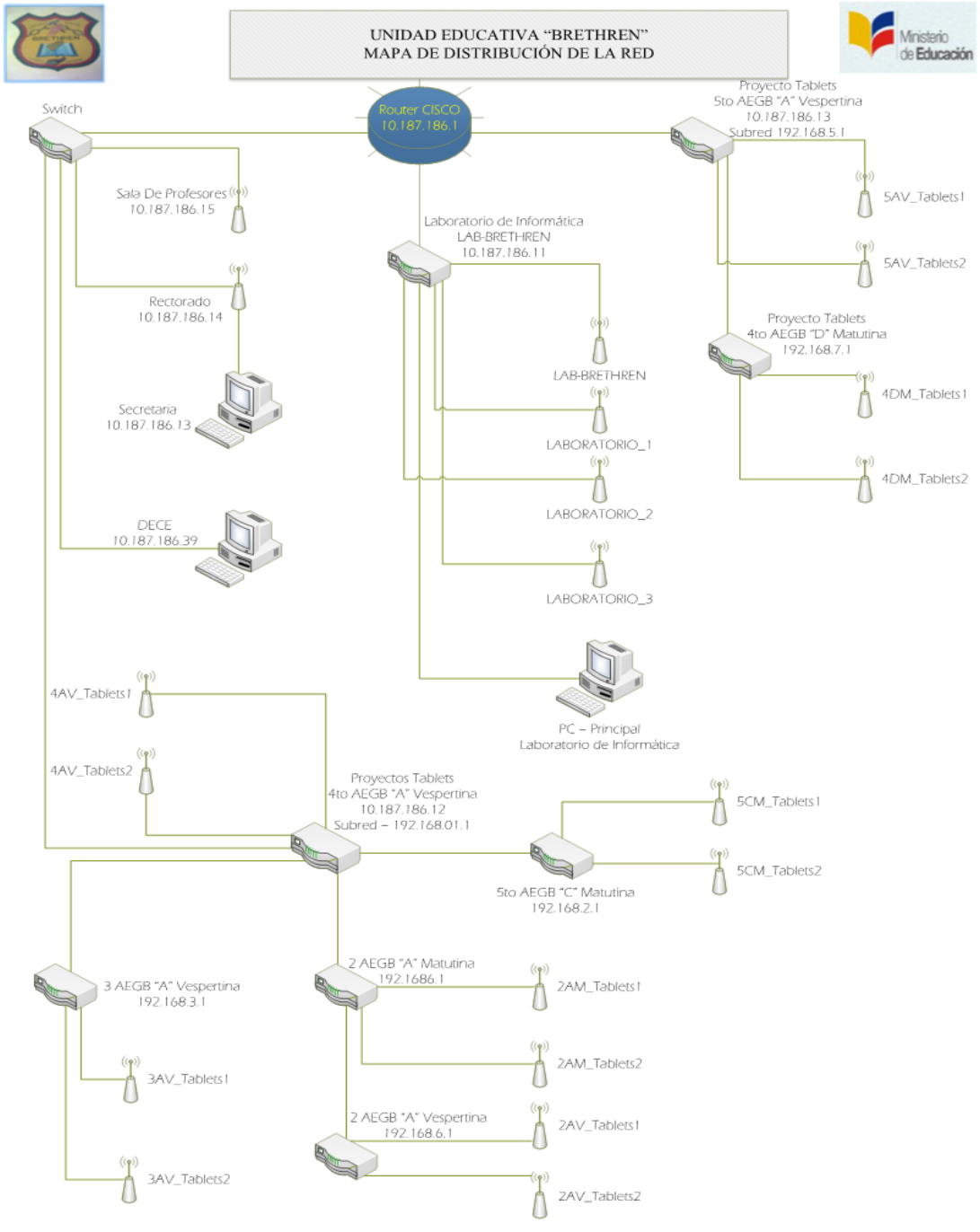


Figura 46: Diseño actual de la red. Diseño institucional

3.6 PROBLEMAS DE SEGURIDAD ENCONTRADOS EN DISPOSITIVOS DE PROTECCIÓN DE LA RED

Durante el análisis se captura el tráfico de la red por 3 días en el PC de laboratorio que está conectado directamente al router principal pero con dirección subneteada, además una captura directa al router en una 4to día, en los cuales los docentes hacen uso de la red casi al 100% (horas pico), según lo analizado existe la sospecha de que hay un envenenamiento ARP ya que la puerta de enlace con dirección 10.187.186.1 pide información a varios host en muchas ocasiones incluyendo los paquetes etiquetados como GRATUITOUS, por ejemplo desde el paquete 27729 de tráfico 26-08-2016 la ip 10.187.186.15 solicita la MAC a 10.187.186.1 y la solicitud continua hasta el paquete 28174 en este caso se consideraría que ya deben conocerse los host para la transmisión con un replay pero luego continua intentando la solicitud, esto está ocurriendo en las tres capturas, cuando el paquete esta con una subred de igual manera solicita en el paquete 34 del 22-08-2016 en la pc principal del laboratorio la ip 192.168.1.209 hace la solicitud a la puerta de enlace de la subred 192.168.1.1, en el paquete 35 ya es entregada la MAC de la IP 209 pero nuevamente la IP 1.1 vuelve a solicitar MAC, en las capturas 26-08-2016 y 24-08-2016 ocurre la misma situación, se asumiría que esto podría ser la petición hacia cada host que está conectado a la red por ser un broadcast pero si ya se conoce una determinada dirección física no es necesario nuevamente solicitudes en forma repetida y constante, Figura 47.

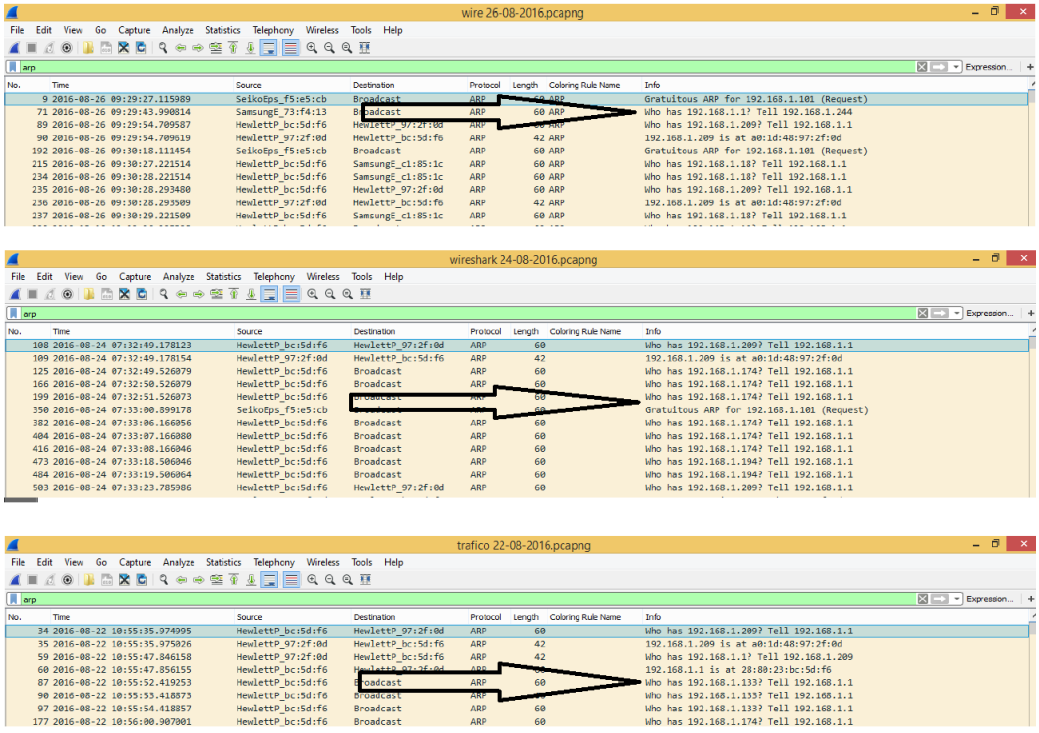


Figura 47: Gráficas de análisis de un posible ataque mediante envenenamiento ARP

En la cuarta captura existen excesivas peticiones ARP de varios host, los cuales la mayoría lo hacen hacia la IP de la puerta de enlace lo que provoca una sospecha de que el router está siendo atacado, no se encuentra segmentos TCP con flags repetidos o con IPS desviadas de sus host correspondientes por lo tanto se descarta un posible DDOS, en el análisis del filtro DNS no se encuentra anomalías aparentemente y en una consulta, sin embargo lo extraño es que en la captura aparecen consultas a dominios que fueron abiertos con anterioridad, no en el momento de la captura, además como se dispone de un firewall IPS SHOPOS deberían existir respuestas de bloqueo a dominios como son youtube.com en

el paquete 8169 y otros pero no se ejecutan dichos bloqueos, haciendo una consulta con el administrador de la red da a conocer que la configuración del IPS firewall solo tiene las configuraciones por defecto, lo que se considera como varios bugs debido a negligencia por parte de los administradores en las configuraciones.

Al utilizar filtros en búsqueda de respuestas ACK con un DNS o puerta de enlace diferentes a lo que entrega por defecto el router 10.187.186.1 o la subred 192.168.1.* con la consulta:

bootp.option.value == 05 && (frame[309:6] != 03:04:c0:a8:fe:fe || frame[315:6] == 06:04:c0:a8:fe:d3), se descarta de un ataque DHCP Spoof empleado por algún DNS ilegítimo.

Un posible ataque que podría darse una inundación de peticiones de direcciones DHCP DISCOVER al router ya que en la infraestructura no se dispone de switchs configurables y no se puede utilizar ACLs sin embargo en el análisis no se encuentra este tipo de anomalías.

Aplicación de un filtro DTP con la intención de un posible cambio de etiquetados en VLANs virtuales o algo parecido sin embargo no se encuentra ninguna respuesta negativa.

Análisis en búsqueda de posibles intrusos malware utilizando exportación de objetos FILE>>EXPORT OBJECT>> HTTP en búsqueda de posibles anomalías descargadas desde la web, sin embargo solo se encontró descargas básicas como imágenes propias de las páginas por lo tanto se descarta intrusos desde el internet.

Se puede descartar un posible ataque de intrusos en forma binaria ya que el IPS instalado bloquea páginas sospechosas desde una base de datos actualizable que contiene, sin embargo

un usuario con conocimientos básicos podría utilizar programas como UltraSurf para engañar al IPS y permitir el acceso a cualquier página sin restricción, como es conocido un ataque binario es difícil de mitigar, se realiza una búsqueda UDP para buscar secuencias de uso por parte de malware sin embargo no hay resultados positivos.

Se reporta por parte del administrador que el ancho de banda que entrega el servicio de internet es de 10MB sin embargo muchas veces durante la jornada hay perdida de conexiones o des anclaje por parte de los host a la red sin motivo alguno o que la tasa de transferencia en ocasiones va en descenso sea en horas pico o horario normal, para lo cual se hace un filtro ICMP en búsqueda de su frecuencia o mensajes de error por parte de este protocolo, pero no hay respuesta positiva de anomalía. Filtro: (icmp.type == 3 && icmp.code == 2) || (icmp.type == 4 && icmp.code == 0)

Se utiliza un filtro en búsqueda de sesiones de redes sociales o páginas que posiblemente entran en la red sin embargo no hay respuesta positiva. Filtro utilizado: http.cookie and http.host contains "facebook", como se realiza un análisis del tráfico y se tiene el apoyo del IPS Sophos no es necesario intervenir en las sessiones TCP sin embargo se lo ha hecho en paquetes con una ligera sospecha de anomalía pero no se ha encontrado ninguna novedad importante como es el caso del paquete 29 TCP.

Por último se hace uso de una herramienta importante denominada EXPERT INFORMATION en la cual si se encuentran muchos problemas desde paquetes mal formados con alta criticidad hasta secuencias encriptadas con problemas de ensamble, aplicaciones que devuelven códigos de error comunes de HTTP, 25 paquetes mal formados

que solicitan retransmisión, finalización de conexiones en los chats entre otros, lo que conlleva a confirmar que la sospecha de ataques mediante envenenamiento ARP o denegación de servicio si se está presentando en determinados tiempos por parte de un host o sistema interno.

CAPÍTULO 4

4.1 PROPUESTA DE DISEÑO DE INFRAESTRUCTURAS PARA PRUEBAS

Según lo analizado en el diseño actual de la red de la Unidad Educativa Brethren se encuentra con problemas de seguridad desde la conexión interna (dispositivos móviles, PCs, conexiones libres a los APs) hasta la externa (internet), no se cuenta con servicios de correo corporativo, web, FTP, existía un portal cautivo proporcionado por el anterior proveedor de internet pero fue dado de baja, etc., la distribución de direcciones IP se las realiza desde el router a los APs[31] disponibles, por lo tanto no hay ningún servidor configurado.

Existe un SPI SOPHOS Fortinet configurado por CNT-EP, con restricciones de rediseño por parte del Ministerio de educación sin embargo mediante Wireshark se han localizado algunos problemas de inseguridad e inclusive instalando aplicaciones en un computador común como por ejemplo nmap para luego conectarlo a la red alámbrica o inalámbrica se puede con facilidad hacerlo correr y lanzar ataques siendo transparente al administrador y al IPS actual.

[31] Puntos de acceso a una red inalámbrica.

Dentro de la red se propone primero realizar un análisis de tráfico mediante Wireshark entre el router y la red para capturar los paquetes entrantes y salientes, localizar errores que se presenten para posterior toma de decisiones respecto a las posibles soluciones que se encuentren, una vez localizados los problemas se pretende colocar en esta misma posición un IPS Snort en el cual se desarrolle una red neuronal embebido en sus módulos de procesamiento para que capture el tráfico, lo analice y posteriormente tome decisiones respecto a su estructura, diseño propuesto Figura 48.

El objetivo de este diseño es localizar anomalías el momento de obtener solicitudes de conexión, durante las cuales se busca analizar las peticiones sean las comunes como es el caso de tree-way-handshake en los cuales lo básico y conocido es negociar la conexión en tres pasos lo que es considerado como tráfico normal, sin embargo si en los casos comunes se da el problema de que las solicitudes sobrepasen las peticiones sea de uno o varios host provocando que las dichas peticiones se las realice en forma exagerada inundando la memoria o provocando colapsos en la misma será considerado como tráfico anormal como es el caso en un ataque DOS (ataques de denegación de servicio) o inundaciones ARP, esto quiere decir que el monitoreo será realizado a nivel de capa 2 (nivel de enlace), por el momento queda expuesto en este proyecto como pruebas de estudio para posterior aplicación.

4.2 DISEÑO Y CONSTRUCCIÓN DE RED DE PRUEBAS PARA PROTECCIÓN

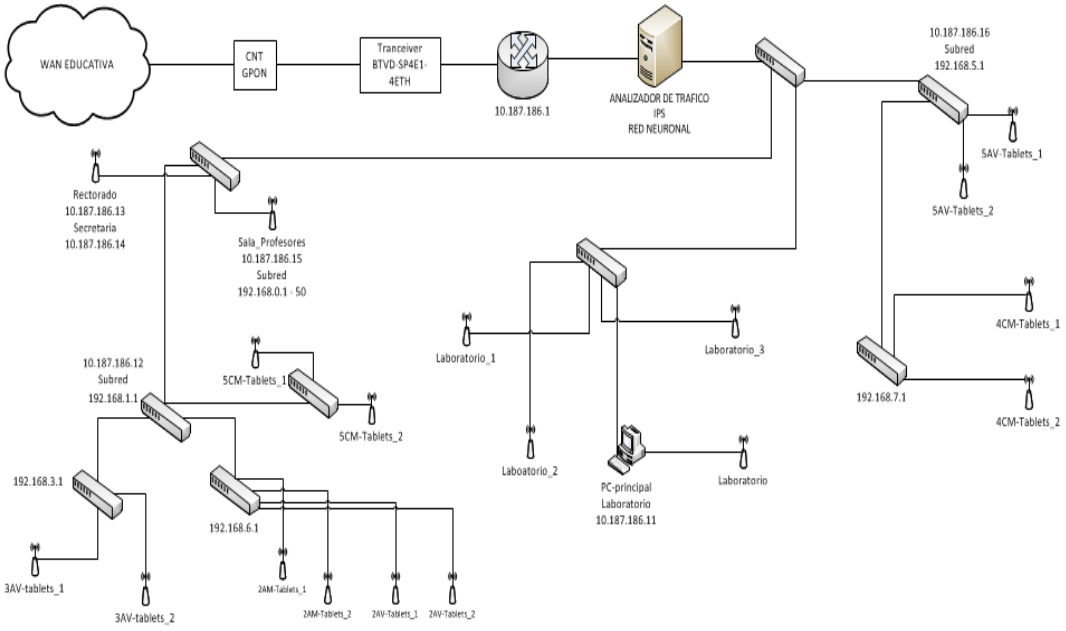


Figura 48: Esquema de pruebas para protección de la red de la institución

Fuente: Diseño Autor

4.2 ANÁLISIS DETALLADO DE RED

La conexión se servicios inician desde la WAN educativa, la infraestructura con los que cuenta la red actual de la institución son proporcionados por el M.E. y los servicios que ha contratado son proporcionados por Telconet y CNT, de esta red se sirve la comunidad educativa, en este caso docentes, padres de familia y estudiantes. Los docentes y autoridades utilizan la red de Sala_Profesores con IP 10.187.186.15 y una subred 192.168.0.1 – 192.168.0.50, la red Laboratorio_2 con IP 10.187.186.11, en la cual tienen servicios de chat mediante aplicación WhatsApp, correo, buscadores y aplicaciones del M.E., además en los

proyectos tablets siguen el uso de aplicaciones educativas Android, los estudiantes hacen uso de la red Laboratorio_2 con aplicaciones educativas pero con bloqueo de servicios youtube, redes sociales y descarga de programas ejecutables, lo cual no se puede establecer como una solución y se pretende quitar esta restricción ya que dicha página dispone de cientos de videos educativos que sirven de apoyo al docente.

El router dispone de tres conexiones hacia los swicths, a lo cual se procederá a colocar 1 computador con 2 tarjetas de red desde la salida del router y antes de la entrada a los switchs, el cual tendrá las siguientes características:

Tabla 4: Características físicas del IPS Snort

COMPONENTES	CARACTERÍSTICAS
Microprocesador	DUAL CORE 1.6 GHZ
Memoria	2 GB
Disco	40 GB
2 Tarjetas de red	3 COM
Sistema Operativo	Ubuntu 12.0
IPS	Snort 2.9

4.2.1 Infraestructura

Equipos CNT y clientes encendidos.

Conexiones de cable de red

Conexiones fibra óptica

Conversor fibra óptica

Router

Switchs

Firewall Sophos

4.2.2 Configuraciones lógicas

Tabla 5: Direcciones asignadas a la Institución por parte de CNT

DIRECCION IP	10.187.186.19
MASCARA DE SUBRED	255.255.254.0
PUERTA DE ENLACE	10.187.186.1
SERVIDOR DNS 1	10.11.11.18
SERVIDOS DNS 2	200.107.10.100

La mayoría de los puertos en esta red están cerrados, sin embargo al router se le puede hacer una conexión remota mediante Telnet lo cual implica que si es descubierta por algún atacante mediante la herramienta Nmap con toda tranquilidad puede ingresar, la instrucción que permite escanear este puerto abierto en la red es #nmap –sP rango de IPs a buscar, con la posibilidad de ser explotado para intrusiones.

Las conexiones a la red se las realizan mediante autenticación de la dirección física configurado en los puntos de acceso inalámbricos y para los casos que no se dispone de autenticación MAC se cuenta con política de contraseñas que son modificadas cada mes, la

mayor parte de acciones realizadas en la red son monitoreadas por la subsecretaria de educación.

4.3 SOLUCIONES A PROBLEMAS DE SEGURIDAD ENCONTRADOS

En el caso del primer problema y del último utilizando herramientas de análisis exhaustivo además de lo mencionado anteriormente se encuentra con posibles modificaciones a la información ya que llega en fragmentos o errónea y las solicitudes de las direcciones físicas son constantes por ejemplo en el caso del paquete 448 al 492 se hace un broadcast por la dirección MAC HewlletP a0:1d:48:97:2f:0d hacia la puerta de enlace, lo cual no es contestado con MAC aproximadamente cada 15 paquetes para luego responder a este llamado la dirección CiscoInc f4:4e:05:bb:86:f8, sin embargo vuelve a hacerse la petición por otros 15 paquetes para luego continuar con otras direcciones físicas en las mismas circunstancias, a esto se le añade que con la herramienta Expert Information se encuentra paquetes modificados, errores de conexión de RST, posibles duplicaciones de direcciones IP, extensiones de imágenes modificadas, retransmisiones de paquetes incompletos o perdidos, conexiones establecidas, interrumpidas, finalizadas para nuevamente ser reconectadas, adicionalmente quejas que existen por parte de todos los usuarios y del administrador de la red que hay desconexiones constantes tanto en el internet como en los servicios básicos se tiene como sospecha que existe un envenenamiento ARP DoS y que está infectando a las redes con IP 192.168.0.* y 10.187.186.*, dando a entender que la infección pasa al router a través de las IP para luego enlazarse con las direcciones MAC, para lo cual la solución propuesta es analizada a continuación:

- Segmentar las redes mediante un switch de gama alta procurando utilizar ACLs[32], VLANs[33] y que disponga de funciones específicas para prevención de ataques.
- Se podría indicar a los sistemas operativos principales de las estaciones de trabajo que la cache ARP va a ser estática, evitando de esta manera que sea actualizada con la información proveniente de la red, previniendo el ataque sin embargo hay que tomar en cuenta que existen muchas conexiones por parte de los integrantes de la institución lo que provocaría es que no se pueda tener conexiones más que para un determinado grupo, la misma situación ocurriría si se permite conexiones estáticas a partir de las direcciones físicas.
- Por último utilización de herramientas que permitan conocer si una o varias tarjetas están en modo promiscuo.
- Hay que tomar en cuenta que debido a la infraestructura y los costos no es posible realizar con facilidad estas implementaciones así que lo que se propone en este caso como solución es un IPS Snort con red neuronal embebida en la configuración de los preprocesadores sfPortscan aplicando alertas de análisis por parte de Nmap, TCP Portscan, TCP Distributed Portscan.

Adicional a lo expuesto es implementar una política de concienciación en las descargas desde lugares conocidos como sospechosos por parte del administrador de red y los usuarios.

[32] Listas de control de acceso
[33] Redes virtuales

4.4 ELECCIÓN DE IPS Y REDES NEURONALES ARTIFICIALES A UTILIZAR

Realizando pruebas en busca de posibles conexiones en varios IPS de software libre adicionales a Snort con lo cual se encontró problemas para implementación como es el caso de ClearOS en este si hay la posibilidad de crear nuevas reglas para identificar diferentes ataques mediante la conexión repetida a un puerto o protocolo como es el caso de DDoS, decoy, envenenamientos ARP, etc., hay la posibilidad de reconocimiento, sin embargo si es necesario un cambio adicional en sus librerías no se puede ya que muchas las tiene codificadas en forma binaria y para obtener soporte de las mismas es necesario registrarse en su página de desarrollo lo cual tiene costos adicionales por cada implementación nueva, no existe documentación abierta respecto a modificación de sus librerías y cabeceras, IPCOP es una buena opción ya que lleva integrado un firewall el cual dispone de herramientas complementarias para reconocer posibles ataques y lleva implementada la estructura del IDS Snort, pero su configuración se centra más en el firewall que en el IDS y como es sabido los ataques internos en una red son su mayor vulnerabilidad queriendo decir que a más de toda la configuración que conlleva IPCOP la posibilidad de crear módulos adicionales es muy pobre.

Hay que tomar en cuenta que para hacer un análisis exhaustivo de todo el tráfico se necesitaría de recursos tanto en hardware como en software robustos para evitar el colapso del IPS ya que un solo paquete de datos genera muchas características Figura 49, para lo cual solo se tomará parte del tráfico basado en el tipo de ataque que se tiene sospecha y su

característica, en este caso el envenenamiento ARP y conexiones SYN por protocolo TCP que está provocando la negación de servicios descritos en el subcapítulo anterior por lo cual también se ha optado un estudio del tráfico por el algoritmo Filtro de Bloom en una matriz de 1 n-gram (2^8 posiciones para pruebas), 3 n-gram es lo que recomiendan, en los mismos serán almacenados las peticiones localizadas con la bandera SYN hacia el protocolo ARP mediante TCP, lo cual será aceptado para que pase a la red neuronal y esta la analice, de no ser así y se encuentre con otro tipo de tráfico el algoritmo desechará la información y continuara con la búsqueda tomando en cuenta que para esto se necesitan los análisis estadísticos y lo recomendable es utilizar el coeficiente de Correlación de Pearson ya que muchas veces se puede cometer el error de escoger datos como falsos negativos de un grupo de información analizado, se puede ir implementando más n-gram para almacenar mayor información pero por lo pronto se realiza pruebas dedicándonos a un solo tipo de ataque evitando la aglomeración de excesiva información en el IPS, tomando en cuenta que lo que se busca es estudiar la conexión de paquetes hacia puertos específicos para indicar al IPS que posibles características de anomalías pueden presentarse durante un ataque, todo esto mediante los resultados que pueda arrojar Snort cuando se presenta un escaneo.

# Campo	# Rasgo	Descripción	Protocolo	Tamaño
1	1	ToS (Tipo de servicio)	IP	1 byte
2	2	Longitud Total	IP	2 bytes
3	3	Banderas	IP	3 bits
4	4	Tiempo de Vida	IP	1 byte
5	5	Protocolo (se refiere al protocolo de nivel superior)	IP	1 byte
6	6	Cantidad de Opciones *(si las hay)*	IP	1 byte
7	7	Tipo	ICMP	1 byte
8	8	Código	ICMP	1 byte
9	9	Puerto Fuente	TCP	2 bytes
10	10	Puerto Destino	TCP	2 bytes
11	11	Número de Secuencia	TCP	4 bytes
12	12	Número de acuse de recibo	TCP	4 bytes
13	13	Banderas	TCP	6 bits
14	14	Ventana	TCP	2 bytes
15	15	Cantidad de Opciones *(si las hay)*	TCP	1 byte
16	16	Puerto Origen	UDP	2 bytes
17	17	Puerto destino	UDP	2 bytes
18	18	Longitud del Mensaje	UDP	2 bytes
19	19-418	Primeros bytes del área de datos (400)	APLIC.	400 bytes
20	419	Tiempo transcurrido desde la llegada del último paquete.	-	4 bytes

Figura 49: Estructura de un paquete con sus características

Fuente: (Fonseca, Pérez, Fernandez, Mora, & Gil, 2014)

A continuación se utiliza el IPS Snort activándolo con la instrucción /Snort – Q utilizándolo en modo “inline” con política config policy_mode: inline lo cual permite manejarlo como un IPS, este tendrá las configuraciones en el preprocesador sfPortscan en la cual será posible la programación de la red neuronal y es el preprocesador más adecuado para el escaneo de puertos al conocerse dos o más direcciones físicas, con lo cual lo hace ideal para implementaciones adicionales en búsqueda de paquetes sospechosos.

Se utilizará una red neuronal procurando la mayor similitud a la de Hopfield ya que el preprocesador Portscan de Snort dispone de una red neuronal integrada para el escaneo de puertos con la intención de aprovechar la recursividad de sus procesos al momento de ajustar los pesos para su aprendizaje.

4.5 CONFIGURACIÓN DE REDES NEURONALES ARTIFICIALES E IPS

4.5.1 Diseño previo a instalación del IPS

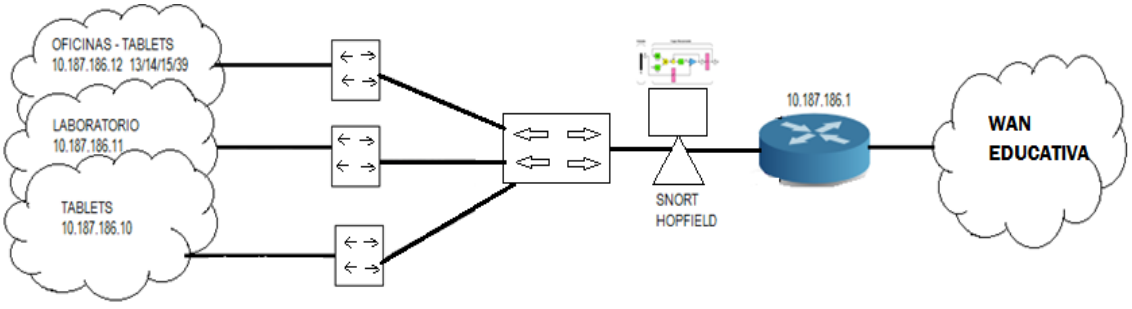


Figura 50: Esquema estructura Hopfield SPI

Fuente: Elaborado por autor.

4.5.2 Configuración de Snort

4.5.2.1 Configuración básica de Snort

Para realizar las pruebas se realiza la configuración previa desde la instalación en software libre sobre el sistema operativo Ubuntu 12 Figura 49, se realiza la instalación con los procesos básicos de Apache2, la instalación de la base de datos mysql incluyendo contraseñas con su respectiva base de datos de nombre snort y la configuración de php5 todo esto tomando en cuenta la configuración de las tarjetas de red eth0 y eth1, de igual forma la configuración básica de las alertas en caso de ingreso a webs que la institución no permite

debido a restricciones por contenido inadecuado todo esto realizado en el fichero snort.conf para la configuración del preprocesador y sites.rules para las posibles alertas Tabla 6.

Tabla 6: Configuración básica de Snort para la creación de reglas (Snort.ogr)

SISTEMA Y APLICACIONES	CONFIGURACIÓN
Ubuntu 12	Configuración de aplicaciones básicas
Apache2	#sudo apt-get install apache2 #sudo /etc/init.d/apache2 restart
Mysql	#sudo apt-get install mysql-server #mysql –u root –h localhost –p mysql> create user'snort'@'localhost' identified by 'contraseña' ; mysql> create databases snort; mysql> grant all privileges on *.* to 'snort'@'localhost'; mysql> flush privileges;
Php5	#sudo apt-get install php5 php-mysql
Snort	#cd /usr/share/doc//snort-mysql/ #sudo dpk-reconfigure –plow snort-mysql #sudo gedit /etc/snort/snort.conf VAR HOME_NET 192.168.0.1/24
etc/sites.rules	#gedit /etc/snort/rules/site.rules

	Configuración de reglas para evitar páginas indeseadas ejemplo: alert tcp $EXTERNAL_NET any -> $HOME_NET any / (msg:"Existe un escaneo con nmap" ;flags:A;ack:o; /reference:arachnids,28;classtype:attempted-recon;sid:628;/ rev:1;)

4.5.2.2 Configuración de los preprocesadores de Snort

Los preprocesadores son módulos que se integran entre el decodificador de tramas y el motor de detección Figura 50., estos se configuran dentro del archivo snort.conf en el paso #3.

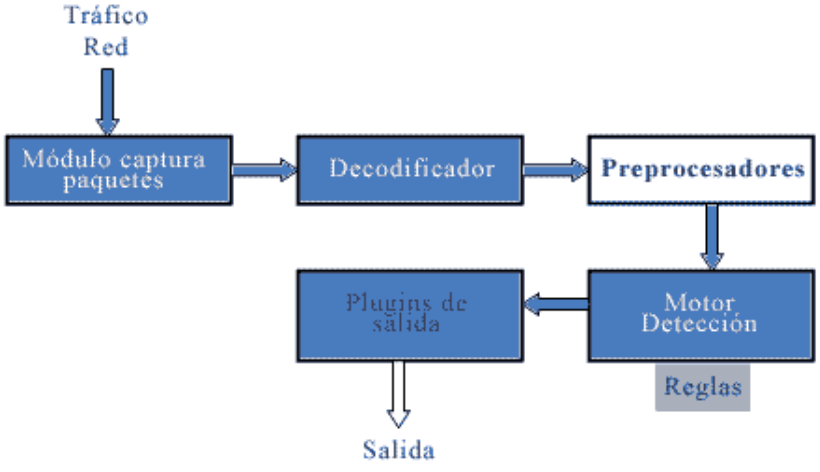


Figura 51: Ubicación de los preprocesadores dentro de Snort

Fuente: (Fernandez, 2009)

En este caso la configuración para reconocimiento de ataques por envenenamiento ARP basado en TCP y SYN se lo hace mediante el preprocesador sfPortscan, tomando en cuenta que hace uso del preprocesador stream5 que viene por defecto activado y es el que permite el reensamblado de paquetes TCP e inspección del estado inspeccionando las conexiones TCP y UDP ya que los ataque no son orientados a la conexión, con la intención de localizar posibles escaneos de puerto durante la captura de tráfico filtrado, que se menciona en el capítulo 3 a través de Bloomfilter, como los preprocesadores poseen las características de módulos del lenguaje C se puede integrar la estructura de la red neuronal basándose en instrucciones de Java ya que tiene mucha similitud con este lenguaje de programación y este es compilado por Snort, a lo mencionado se presenta la estructura del preprocesador sfProtscan:

preprocessor sfportscan: proto < all >

scan_type <portscan | portsweep |decoy_portscan |distributed_portscan | all>

sense_level <low |medium | high>

watch_ip <IP o IP/CIDR>

ignore_scanners <IP lista>\

ignore_scanned <IP lista>

logfile <ruta y nombre del archivo>

Tabla 7: Directivas de la estructura sfPortscan (Fernandez, 2009)

proto < >	Es el protocolo que se desea utilizar TCP, UDP, IP etc.
scan type < >	Tipos de escaneo que se desea utilizar
sense_level < >	Representa el escaneo a utilizarse
watch_ip	Indica que redes se va a inspeccionar
ignore_scanners < >	Ignora las IPs, redes o puertos considerados como escáner activos
ignore_scanned < >	Ignora las IPs, redes o puertos que son objetivo de un escaneo
logfile < >	Nombre del archivo donde Snort guardará los logs de las alertas
memcap < >	Cantidad de memoria a utilizar sfPortscan expresada en bytes
Conection count/IP count	Indica promedio estimados de conexiones por IP
Conection count/port count	Indica la relación entre conexiones por puerto

Ya descrita la estructura la configuración más adecuada para el preprocesador es:

preprocessor sfportscan: proto < TCP >

scan_type <portscan>

variable# = sense_level<medium>

watch_ip <IP>

logfile <..\snort\logs>

memcap <100>

La configuración descrita se justifica indicando se realizan pruebas, buscando evitar el uso excesivo del tráfico y se utiliza un solo protocolo en busca de posibles escaneos, posteriormente si las pruebas son exitosas se adicionará más protocolos como UDP y la memoria aumentará de acuerdo a los resultados obtenidos, además hay que tomar en cuenta que se va a implementar una red neuronal lo cual puede provocar errores posteriores, de igual forma en watch_ip <IP> se utilizará direcciones de host cercanos al router con la intención de realizar pruebas iniciales, a continuación se irán incrementando las direcciones IP a medida que las pruebas den respuestas positivas, todo esto basado en el preprocesador Stream5 que es el que captura sesiones de escaneos ACK mediante la directiva detect_ack_scan.

4.5.3 Configuración red neuronal Hopfield

Para la configuración de la red neuronal hay que tomar en cuenta que se necesita de un patrón a llenarse para que la red neuronal se active y ajuste los pesos necesarios, esto quiere decir que se necesita de un contador de tráfico en este caso para asignar estos datos al patrón de la red Hopfield dentro del preprocesador la directiva que asigna los conteos mencionados es *Conection Count* o *IP Count* mostrando el promedio estimado de conexiones por IP y la relación entre conexiones por puerto para este caso lo más recomendado para pruebas es

Connection Count ya que lo que interesa en este caso es saber cuántas conexiones realiza el protocolo ARP en los puertos que solicita mediante ARP request, por ejemplo si se da el caso de la instrucción: nmap –sS –sV -P0 192.168.0.* o 10.187.186.* dentro de la red institucional, relación tomada de las probabilidades de salida entre el IPS (Fernandez, Snort. Preprocesadores. SfPortscan., 2010) y el tráfico analizado en capítulo 3.

El patrón inicia de la siguiente manera:

- 3 vectores i de entrada con 10 j elementos en los cuales se inicializan las posibles conexiones a los puertos.
- Una matriz de pesos de 30 i, j para ajustar de acuerdo al número de datos que se van a comparar en el momento que ingresa el tráfico y que relaciona directamente por el número de conteos mencionados en conection count dentro de la configuración de Snort, de acuerdo a la muestra.
- La idea básica es que si la directiva *connection count* supera un límite de conexiones por ejemplo; según un ataque ya establecido con #nmap –sS –sV –PO 192.168.1.5 arroja 15 conexiones al puerto desde una dirección X.X.X.X a una spoofeada 192.168.1.5, lo que quiere decir es que si sucede un caso similar a la dirección 10.187.186.1 que es la puerta de enlace se considera que hay una posible petición fuera de lo común lo que quiere decir que es un falso positivo con alteración de entradas, tomando esto como ejemplo para posteriormente realizar el resto de host.

  fil1 = [1,1,1,1,1]

  fil2= [1,1,1,1,1]

fil3= [1,1,1,1,1]

Cada uno de los patrones predefinidos como representación de una conexión a los puertos para lo cual si la entrada intentó realizar una conexión se compara con los patrones fil1, fil2, fil3, en los cuales puede ser un patrón completo o parte de él comparado con las entradas se considera como un ataque.

- Patrones de entrenamiento y aprendizaje
- Lectura del tamaño de la matriz patrón se completa con -1 para poder crear la matriz identidad.

  int [][] matriz = {{1,1,1,1},{1,1,1,1,1},{1,1,1,1,1},{-1,-1,-1,-1,-1},{-1,-1,-1,-1,-1}};
- Una sola neurona para el aprendizaje lo que significa que se ahorra programación.
- ETAPA DE APRENDIZAJE

  Algoritmo de Hopfield

  Definición de la matriz identidad de tamaño 5*5

  ```
  int j;
  int [][]I = new int[5][5];
  for (i=0;i<5;i++)
  for (j=0;j<5;j++)
  if (i==j)
  I[i][j]= 1;
  ```

else

I[i][j] = 0;

- Para cada patrón calcular la matriz de pesos de acuerdo a la formula $W = \sum (E \cdot E^T - I)$

int[][]W = new int[5][5];

for (i=0;i<M;i++) {

int [][]T = new int[5][1];

int [][]Ei = new int[1][5]; }

for (j=0;j<N;j++) {

Ei[0][j]= E[i][j];

matriz.traspuesta(Ei,1,5,T);

int [][]P = new int[5][5];

matriz.producto(T,Ei,5,5,1,P);

int [][]OP = new int[5][5];

matriz.opuesta(I,5,5,OP);

int [][]S = new int[5][5];

matriz.suma(P,OP,5,5,S);

matriz.suma(W,S,5,5,W);

}

- ETAPA DE FUNCIONAMIENTO

  Se captura el tráfico desde el preprocesador y se realiza los conteos de los escaneos a los puertos.

  int[][]Ent = new int[1][5];

- Lectura de la entrada Entrada

  cont=0;

  for (f=0;f<fil;f++)

  for (c=0;c<col;c++)

  Ent[0][cont++] = Terminal.leeEntero(conection count);

- Calcula una nueva salida mientras sea distinta de la anterior salida

  int [][]S = new int[1][5];

  boolean igual=false;

  do {

- Aplicacion de la función escalón con desplazamiento 0

  matriz.producto(Ent,W,1,4,4,S);

- Transformación de los valores de la salida S a valores discretos 1, -1

  for (j=0;j<N;j++)

  if (S[0][j]<0)

  S[0][j]= -1;

  else

  S[0][j]= 1;

- Comparación de las salidas en t y (t+1)

  if (matriz.iguales(Ent,S,1,4))

  igual=true;

  else

- La salida es la nueva entrada

  for (j=0;j<N;j++)

  Ent[0][j] = S[0][j];

  } while (!igual);

- Alerta de escaneos

  alert tcp any any -> $HOME_NET any (content:"|00 01 86 a5|"; msg: "Posible ataque mediante scaneo de puertos";) log tcp any any -> $HOME_NET any (msg:"escaneos tcp"; sid:10000001;)

- Clases para las matrices
- Devuelve en T la matriz traspuesta de A, f,c representan el número de filas y de columnas de A

  public static void traspuesta(int [][]A,int f,int c,int [][]T) {

  int i,j;

  for (i=0;i<f;i++)

  for (j=0;j<c;j++)

  T[j][i]=A[i][j]; }

```
public static void producto(int [][]A,int [][]B, int Af, int Bc, int cf,int [][]P) {
int i,j,k;
for (i=0;i<Af;i++)
for (j=0;j<Bc;j++)
for (k=0;k<cf;k++)
P[i][j] += A[i][k] * B[k][j];
}

public static void opuesta(int [][]A ,int f, int c,int [][]OP) {
int i,j;
for (i=0;i<f;i++)
for (j=0;j<c;j++)
OP[i][j]=-A[i][j];
}

public static void suma(int [][]A,int [][]B,int f, int c,int [][]S) {
int i,j;
for (i=0;i<f;i++)
for (j=0;j<c;j++)
S[i][j]=A[i][j] + B[i][j];
}
```

```
public static boolean iguales(int [][]A,int [][]B, int f, int c) {
int i,j;
boolean igual=true;
for (i=0;i<f;i++)
for (j=0;j<c;j++)
if (A[i][j]!= B[i][j])
return (false);
return (igual);
}

public static int posminimo(double []A) {
int i, pos=0, size;
double valminimo;
valminimo= A[0];
size= A.length;
for (i=1;i<size;i++)
if (valminimo > A[i]) {
valminimo=A[i];
pos=i;
}
```

```
return (pos);
}
int i,j,m;
double k;
double []B= new double [f];
for (i=0;i<f;i++)
if (i==x)
continue;
else {
for (m=0;m<f;m++)
B[m]= M[m][y];
k= - M[i][y];

for (j=0;j<c;j++)
M[i][j] += -M[x][j] * B[i];
}
}

public static void Gauss(double [][]M,int f,int c) {
int i,j,k;
double []B= new double [c];
```

```
for (i=0;i<(f-1);i++)
for (k=i+1;k<f;k++){
for (j=0;j<c;j++)
B[j]= -M[k][i]* M[i][j] + M[i][i]*M[k][j];
for (j=0;j<c;j++)
M[k][j] = B[j];
}
}
```

Algoritmo basado en estudios de hopfield de (Andaluza, 2000)

4.5.4 Diseño de políticas.

Una política es establecer la detección de anomalías de TCP mediante el preprocesador Stream configurándolos a través de detect_anomalies dentro de snort.conf.

Se puede utilizar el preprocesador Portscan para detectar y alertar un escaneo de puertos el momento que un ataque intente utilizar Nmap para escanear TCP Portscan, de igual forma se puede detectar un escaneo TCP decoy Portscan, de igual manera cuando se intenta hacer un ataque distribuido como es el caso de TCP Distributed Portscan

- Políticas de seguridad

En las políticas de seguridad expuestas para la Unidad educativa Brethren, las autoridades deberán proporcionar los procedimientos internos mediante una comisión que permita su revisión y actualización, estos deberán tener las características esenciales que a continuación se detallan.

- Definición de la seguridad de la información, objetivos, alcances generales y la importancia de la seguridad para la institución.
- Declarar el propósito de las autoridades responsables y el administrador de la red, apoyando los principios y objetivos de la seguridad de la información.
- Una breve explicación de las políticas, principios, normas y requisitos de cumplimiento de la seguridad entre estos son:

a) El cumplimiento de los requisitos legales que deben ser difundidos a toda la comunidad.
b) Formas de prevenir y detectar virus y software malicioso que deberá ser difundido por el administrador de la red.
c) Consecuencias de las violaciones a las políticas de seguridad que fueron desarrolladas.
d) Definición de responsabilidades generales en lo que respecta a materia de seguridad.
e) Referenciar documentos que respaldan las políticas de seguridad que deber cumplir los docentes, autoridades, estudiantes y padres de familia.

De acuerdo a lo mencionado se establecen las políticas para uso de la red dentro de la institución:

a) Instalación de software: El software que deberá ser instalado en los equipos de la Unidad Educativa Brethren es el siguiente:

- Sistema Operativo (Windows 8.1 o Android en caso de las tablets)
- Antivirus

- Suite Ofimática
- Sistema de Plataforma del ME[34] para consulta, alta y baja de notas de los estudiantes.
- WhatsApp para comunicación interna y externa entre la comunidad educativa.

Utilización de software adicional

En caso de necesitar instalar alguna aplicación adicional fuera de lo que se le entrego con su respectivo deberá hacer una solicitud dirigida a la autoridad correspondiente justificando la necesidad de la instalación.

Cuentas de usuario para el ingreso a la plataforma y conexión hacia la red.

Los docentes, estudiantes y padres de familia deberán contar con un usuario y contraseña proporcionados por el administrador a la red, la cual le permitirá el ingreso a la plataforma del ME, y si desea conectarse a la red solicitar el ingreso mediante direcciones físicas de ser necesario con su respectiva justificación.

Los docentes serán los únicos con privilegios para poder ingresar a información de redes sociales como WhatsApp, con el objetivo de establecer comunicación constante dentro del plantel.

Cada computador, Tablet, o teléfono celular se le asignara un ingreso mediante su dirección física para que pueda acceder a la red.

[34] Ministerio de Educación del Ecuador

Políticas de restricción de los Recursos de la red

Se otorga a los usuarios de la red privilegios para que puedan dar uso a la información en forma limitada que permita en estos obtener capacitación, jerarquización, especialización en sus conocimientos y prácticas que le permita lograr el mayor provecho de los recursos informáticos.

La utilización de los recursos de la red pueden ser revocados o limitados en cualquier momento por razones operativas de actualización o modificación de dispositivos en la red, tomando en cuenta que el uso de estos recursos se encuentran bajo en estricto control permanente de las autoridades.

Utilización indebida de los recursos de la red

Queda explícitamente considerado como uso indebido:

- Realizar cambios o modificar la posición de los equipos, software, estructuras de la información sin la debida autorización por parte de máxima autoridad de la institución.
- Violar o evitar las verificaciones de identidad o cualquier sistema de seguridad.
- Realizar cualquier actividad que intervengan con intereses personales.
- Acceder al código fuente de cualquier software que intervenga en los procesos regulares del plantel.
- Leer información que pertenezca a otros usuarios sin el debido permiso.
- Difundir indebidamente información privada o pública debido a su posición, actividad o función que desempeña.

- Intentar acceder a áreas restringidas de los Sistemas de Información dentro de la estructura informática de la red.
- Intentar descifrar claves, sistemas o algoritmos que intervengan en la seguridad de la estructura informática de la institución.

Uso prohibido

Queda terminantemente prohibido la sustracción de equipos, periféricos que no hayan sido asignados al personal.

- Grabar, modificar o borrar software que no estén incluidas dentro de las labores propias del personal docente.
- Realizar modificaciones en las configuraciones de los equipos que no estén asignados al personal respectivo.
- Acceder a los sistemas de información de los diferentes departamentos sin la debida autorización.
- Enviar cualquier información que haya sido interceptada en fraudulenta.
- Acceder, descargar distribuir o almacenar música, videos, audios, imágenes, documentos que no tengan ninguna relación a la responsabilidad laboral.

Responsabilidades

- Ningún usuario puede utilizar identificaciones, firmas electrónicas, contraseñas o usuarios, aun teniendo la autorización de los propietarios.
- Cada uno de los usuarios es responsable de mantener sus cuentas y contraseñas a buen recaudo evitando revelar sus datos de identificación a otro.

- Si un usuario sospecha que se está haciendo uso de sus datos de identificación por parte de otro debe cambiarlas inmediatamente e informar a la administración.

4.5.5 Decisiones técnicas

4.6.5.1 Situación de la Redes Neuronales Artificiales elegida

Tomando en cuenta que se va a utilizar la red neuronal de Hopfield es necesario solicitar equipo adicional mencionado en el capítulo 3 el cual se ubique al inicio de la red como equipo Front – End compartiendo los recursos del mismo con el respectivo IPS o sensor asignado, esta red será diseñada, configurada y entrenada con anterioridad por parte de la administración, se implementa mecanismos de identificación y adaptación del tráfico capturado por parte de Hopfield embebido en el respectivo IPS y este a la vez tome las decisiones correspondientes.

4.6.5.2 Elementos físicos a utilizar

En la red se adiciona equipos que intervienen en el tráfico de esta, ante lo se utilizará:

1 PCs mínimo DUAL CORE con memoria RAM de 2 GB y 40 GB en disco.

2 tarjetas de red 100/100.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Filtrar información proveniente de una red es una tarea ardua pero muy necesaria si se desea establecer seguridades dentro de cualquier institución, sin embargo existen herramientas informáticas que permiten hacerlo con facilidad, en este caso el hecho de que en la actualidad los antivirus no tienen disponibilidad de respuesta rápida y actualizaciones pobres o nulas ante un ataque es indispensable utilizar mecanismos de análisis de tráfico rápidas y que puedan tomar decisiones en los instantes de una infiltración, para ello el uso de las redes neuronales se ve como mejor opción ante los intensos ataques que en la actualidad sufren las redes, si se combina esta técnica con un IPS se da en principio una idea de seguridad adecuada, sin embargo hay que tener en cuenta que los atacantes están siempre analizando tráfico en búsqueda de fallas tanto en los sistemas operativos como en la estructura de los dispositivos que reciben datos por ello es importante invertir en seguridad, pero no todo es inversión en infraestructura ya que se puede disponer de los mejores equipos en transmisión de datos y los mejores antivirus que el mercado disponga pero si no se tiene políticas adecuadas para el manejo de la información la seguridad se verá comprometida en todo momento, siendo la red blanco de ataques inclusive por los mismos integrantes debido a la poca educación que se tiene acerca de cómo evitar un ataque o falta de pericia al momento de estar siendo blanco de un ataque.

Hay que tomar en cuenta que varias de las investigaciones analizadas describen como se estudia el tráfico para reducirlo tomando en cuenta sus estadísticas de ingreso, características de paquetes y conexiones en el IPS, pero no existe una investigación con la opción de conexión entre el IPS y la red neuronal, lo cual quiere decir que en este trabajo se pretende iniciar pruebas reales con algoritmo y código que posteriormente puede ser ampliado a medida que se sigue realizando estudios de Snort.

Disponer de varias técnicas de análisis y escaneo de tráfico en una red permite que esta pueda funcionar con normalidad sin comprometer la privacidad de la información, hay que tomar en cuenta que dichas técnicas deben ser analizadas con minuciosidad ya que se corre el riesgo de comprometer el rendimiento de la red y sus dispositivos, el hecho de disponer herramientas con código abierto es una buena opción sobre todo en las entidades públicas donde los recursos suelen ser muy limitados, existiendo en la web aplicaciones que pueden ser modificadas de acuerdo a las necesidades de la empresa es conveniente estudiarlas y hacer uso de estas más aún en la actualidad donde la inteligencia artificial es un plus importante y está a la disposición de todos los usuarios.

5.2 Recomendaciones

El momento de establecer reglas de seguridad, se realiza un análisis minucioso de las políticas implementadas en la institución que de los privilegios necesarios a los departamentos correspondientes de acuerdo a la información que cada uno de estos utilice y a la ves que no limite exageradamente la transmisión del tráfico, permitirá tomar las medidas necesarias y a tiempo para evitar desastres, tomando en cuenta que se debe hacer conocer al

personal acerca de que tipos de ataque sufre en la actualidad toda red, ventajas y desventajas que se obtienen de aplicar las políticas de seguridad, las técnicas utilizadas actualmente por los atacantes para acceder a la información de cada usuario procurando evitar la paranoia, dando a conocer las bondades del uso de las redes neuronales combinadas con el SPI y educando a los usuarios acerca de cómo manejar eventos en que se esté viviendo una intrusión, todo esto permitirá que la seguridad se maneje con la responsabilidad que ello requiere y con la ayuda del mismo personal se podrá mantener la confidencialidad de los datos de la institución.

En el mercado comercial al momento se están utilizando técnicas similares a las vacunas en el ser humano en las cuales la inteligencia artificial es la columna vertebral para este tipo de estrategias, es recomendable introducirse en este campo lo que permitirá a cualquier desarrollador encontrar más y mejores soluciones, hay que tomar en cuenta que si a un paquete ICMP se lo envía a la red sin indicarle un TTL este puede permanecer mucho tiempo sin desaparecer, se puede iniciar con esa idea paquetes que modifiquen tráfico con anomalías de poder controlar sus instrucciones.

Lista de referencias

Acosta, M., Salazar, H., & Zuluaga, C. (2000). *Tutorial de Redes Neuronales*. Obtenido de Universidad Tecnológica de Pereíra : http://proton.ucting.udg.mx/posgrado/cursos/idc/neuronales2/

Alba, E. (2005 - 2013). *Lenguajes y ciencias de la computación.* Obtenido de Universidad de Malaga: http://www.lcc.uma.es/~eat/services/fddi/fddi.htm

Albanés, D., & García, L. (30 de septiembre de 2011). Controlador Gestual Basado en Redes Neuronales. Madrid, España.

ALBARRAN, G. B., & GARDUÑO, N. G. (2010,pg. 45 - 47). ARQUITECTURA DE MONITOREO EN TIEMPO REAL DE UNA RED. *TRABAJO FINAL DE GRADO PREVIO A OBTENER EL TITULO DE INGENIERO EN COMUNICACIONES Y ELECTRÓNICA*. México, México. Obtenido de http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/8026/1/ice%20304.pdf

Aliyev, E. (08 de febrero de 2015). *CommunityHelpWiki*. Obtenido de IptablesHowTo: https://help.ubuntu.com/community/IptablesHowTo

ALVAREZ, B. L. (2005, p. 11). "SEGURIDAD EN INFORMÁTICA (AUDITORÍA DE SISTEMAS)". *Trabajo previo realizado para la bbtención del título de Maestro en Ingeniería de Sistemas Empresariales*. Mexico. Obtenido de http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

Andrade, E. (Febrero de 2013). "ESTUDIO DE LOS PRINCIPALES TIPOS DE REDES NEURONALES Y LAS HERRAMIENTAS PARA SU APLICACIÓN". *Tesis previa a la obtención de Ingeniero en Sistemas*. Cuenca, Ecuador. Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/4098/1/UPS-CT002584.pdf

Arredondo, T. (15 de mayo de 2012). *Universidad Técnica Federico Santamaria.* Obtenido de Departamento de Electrónica: http://profesores.elo.utfsm.cl/~tarredondo/info/soft-comp/Introduccion%20a%20las%20redes%20neuronales.pdf

Astudillo, J., Jimenez, A., & Ortiz, F. (2011). ADAPTACIÓN DEL IDS/IPS SURICATA PARA QUE SE PUEDA CONVERTIR EN UNA SOLUCIÓN EMPRESARIAL. *Trabajo previo a la obtención del título de Ingeniero en Ciancias Computacionales Especialización Sistemas de Informacion*. Guayaquil, Ecuador. Obtenido de https://www.dspace.espol.edu.ec/bitstream/123456789/19502/2/tesina_seminario0.6.pdf

Barba, G. (Octubre de 2009). Detección de ataques en una Intranet utilizando Redes Neuronales. *Tesis de grado previa a la obtención de título de ingeniero en informática y ciencias de la computación*. Quito, Ecuador. Obtenido de http://repositorio.ute.edu.ec/bitstream/123456789/5696/1/39780_1.pdf

Barrero, S. (26 de febrero de 2014). Como funciona el cerebro. *Mas allá de la formación*. Obtenido de https://santiagofbarrero.wordpress.com/2014/02/26/cmo-funciona-el-cerebro-qu-es-y-cmo-funciona-la-mente-ii/

BECERRA, I. (Octubre de 2001). Simulación de la Maquina de Inducción Utilizando las redes Neuronales. Quito, Pichincha, Ecuador. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/5441/1/T1853.pdf

BELTRÁN, B. F. (2015). HACKING ÉTICO PARA DETECTAR FALLAS EN LA SEGURIDAD INFORMÁTICA DE LA INTRANET DEL GOBIERNO PROVINCIAL DE IMBABURA E IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), BASADO EN LA NORMA ISO/IEC 27001:2005. *TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN.* Ibarra, Ecuador. Obtenido de http://repositorio.utn.edu.ec/bitstream/123456789/4332/1/04%20RED%20045%20TESIS.pdf

Benítez, J. (19 de Septiembre de 2014). *slideshare.net.* Obtenido de http://es.slideshare.net/jcbp_peru/utp-sirns4red-perceptron

Borja Merino Febrero, I. (febrero de 2011). ANÁLISIS DE TRÁFICO CON WIRESHARK. *INTECO-CERT*. España. Obtenido de https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

Caballero, A. E. (febrero de 2015). Hacking con Kali Linux. *KALI LINUX PENETRATION TESTING, RE-DEFINED*. Lima, Perú. Obtenido de http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf

Calderón, J. L. (febrero de 2003). Red de Hamming. México, México. Obtenido de http://es.slideshare.net/mentelibre/red-neuronal-de-hamming?from_action=save

Calizaya, J. (6 de abril de 2014). *Prezi.* Obtenido de Protocolo HDLC: https://prezi.com/9jjlzajs1fwi/protocolo-hdlc/

Carlson, J. (01 de Diciembre de 2015). *Security Inteligence*. Obtenido de https://securityintelligence.com/ibm-security-returns-to-leadership-position-in-2015-gartner-magic-quadrant-for-intrusion-prevention-systems/

Castillo, J. C. (12 de abril de 2015). *Slideshare.* Obtenido de http://es.slideshare.net/Juancarloslizardcastillo/protocolos-de-capas-inferiores-46909763

Chanaluisa, D., Meza, A., & Tasipanta, J. (2012). IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN Y ADMINISTRACIÓN DE SEGURIDAD PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA UNIVERSIDAD CENTRAL DEL ECUADOR. *TRABAJO DE GRADUACION PREVIO A LA OBTENCIÓN DE TITULO DE INGENIERO EN INFORMATICA.* Quito, Ecuador. Obtenido de http://www.dspace.uce.edu.ec/bitstream/25000/365/1/T-UCE-0011-19.pdf

Chayan, S. (9 de septiembre de 2009, p. 3, 4). Three-way handshaking. *Connection Establishment in TCP*. Bombay. Obtenido de https://e-nautia.com/hichasoft/disk?p=655015

cisco. (2007). *CISCO*. Obtenido de http://www.cisco.com/c/en/us/td/docs/ios/at/configuration/guide/12_4/atk_12_4_book/overview_appletalk.pdf

Cruz Erik, R. D. (2010). MODELO DE SEGURIDAD PARA LA MEDICIÓN DE VULNERABILIDADES Y REDUCCION DE RIESGOS EN REDES DE DATOS. *Trabajo de grado presentado como requisito para obtener el Título de Ingeniero en Informática. INSTITUTO POLITECNICO NACIONAL*. México, México. Obtenido de http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/8428/1/IF2.52.pdf

Cruz, M. (3 de abril de 2011). *marckoz-redes-45trabajo*. Obtenido de http://marckoz-redes-45trabajo.blogspot.com/2011/04/tcpip-ipxspx-netbeui.html

Daza, S. (02 de Mayo de 2003). *monografias.com.* Obtenido de http://www.monografias.com/trabajos12/redneuro/redneuro.shtml

Dragorn. (10 de Julio de 2004). *kismetwireless.* Obtenido de Kismet: https://www.kismetwireless.net/presentations/5hope-kismet.pdf

Enguita, J. M. (junio de 2009). *Universidad de Oviedo.* Obtenido de ISA: http://www.isa.uniovi.es/docencia/redes/protocolos_seguros.pdf

Flores, H. (11 de 06 de 2013). *Instituto Politécnico Nacional*. Obtenido de Polilibro Redes Neuronales Artificiales: http://www.hugo-inc.com/RNA/Unidad%204/4.2.1.html

Flores, H. (11 de Junio de 2013). *Instituto Politécnico Nacional - Escuela Superior de Computo*. Obtenido de Polilibro Redes Neuronales Artificiales 1: http://www.hugo-inc.com/RNA/Unidad%203/3.2.1.html

Fonseca, I., Pérez, F., Mora, R. F., & Gil, J. (29 de Julio de 2014). *dtic.ua.ec.* Obtenido de https://www.dtic.ua.es/grupoM/recursos/articulos/JDARE-08-H.pdf

Gallón, Á. R. (16 de 2013 de mayo). Modo de Transferencia Asíncrona (ATM). *Sistemas de conmutación*. Popayán, Colombia. Obtenido de http://dtm.unicauca.edu.co/pregrado/conmutacion/transp/7-ATM.pdf

García, F. (2005). *Universidad de Huelva.* Obtenido de FUNDAMENTOS BIOLÓGICOS DEL APRENDIZAJE Y LA MEMORIA : http://www.uhu.es/francisco.cordoba/asignaturas/FBAM/TEMAS%20PDF/3-LA%20NEURONA.pdf

García, J. (Dirección). (2012). *Introducción a las redes neuronales para no expertos [VIDEO]* [Película]. Obtenido de https://www.youtube.com/watch?v=uEIpuyUNvuA&spfreload=10

García, M. I. (2008). Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral. *Universidad de Almería Trabajo de grado presentado como requisito para obtener el Título de Ingeniero en Informática*. Almería, Andalucía, España. Obtenido de http://www.adminso.es/recursos/Proyectos/PFC/PFC_marisa.pdf

García, N. (2 de junio de 2012). *Slide Share*. Obtenido de Protocolo TCP/IP: http://es.slideshare.net/neligarciaboc/protocolo-tcpip-13176705

García, N. (2013). *miclase-online.com.* Obtenido de http://www.miclase-online.com/tutoriales/computacion/redes/AEMRedes2.pdf

Guimi. (Abril de 2009, p. 14). *guimi.net.* Obtenido de http://www.monografias.com/trabajos-pdf2/redes-comunicaciones/redes-comunicaciones.pdf

Hernandez, P. M. (2006, p. 44). "Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial". *Trabajo de grado previo a la obtención del titulo de Auditor en control de gestión.* Guayaquil, Ecuador. Obtenido de http://core.ac.uk/download/pdf/12401004.pdf

Hjelmvik, E. (2009). *networkminer.sourceforge.* Obtenido de http://networkminer.sourceforge.net/documents/Network_Forensics_Workshop_with_NetworkMiner.pdf

Horat, D., & Cañizales, J. (19 de abril de 2006). *DavidHorat.com*. Obtenido de http://es.davidhorat.com/publicaciones/descarga/hopfield.pdf

Householder, A. (11 de Noviembre de 2014). *CERT Software Engineering Institute*. Obtenido de Vulnerability Discovery for Emerging Networked Systems: http://cert.org/blogs/certcc/post.cfm?EntryID=209

Isasi, P. (1996). *Modelos Neuronales Competitivos Kohonen & ART.* Madrid: Universidad de Coruña. Obtenido de http://ruc.udc.es/dspace/bitstream/2183/9444/1/CC_019_art_6.pdf

Iza Gustavo A, C. A. (30 de 10 de 2009). Modelo Ontológico de detección y prevención de Intrusiones Basado en Sistemas Multi Agente e inteligencia computacional. *Universidad de Caldas, 4*, 38-49. Colombia. Obtenido de http://vector.ucaldas.edu.co/downloads/Vector4_5.pdf

Izaurieta, F., & Saavedra, C. (11 de enero de 2006). *Universida de Tarapacá.* Obtenido de http://www.uta.cl/charlas/volumen16/Indice/Ch-csaavedra.pdf

Jimenez, M. (24 de diciembre de 2013). *hackpalyers*. Obtenido de Tcpdump: http://www.hackplayers.com/2013/12/que-deberiamos-saber-sobre-tcpdump-1.html

José, D. B. (1 de 09 de 2010). Intrusiones en redes de datos con captura distribuida y procesamiento estadístico. *Trabajo de grado para obtener el título de Magister en Redes de Datos.* Buenos Aires, Buenos Aires, Argentina. Obtenido de http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Britos_Jose_Daniel.pdf

Justicia, P. G. (25 de enero de 2006). Redes de altas prestaciones FRame Relay. Ciudad Real, España.

Kaneria, D. (17 de septiembre de 2012). *Slide share.* Obtenido de IEEE 802.4: http://es.slideshare.net/chromeboyz/token-bus-12864104

Knopf, M. M. (1 de febrero de 2005). *darkstat − Un analizador de tráfico de red.* Obtenido de linuxfocus.org: http://www.linuxfocus.org/Castellano/Archives/lf-2004_09-0346.pdf

León, H. R. (2012). Definición de un Modelo de Seguridad en Redes de Cómputo mediante el uso de técnicas de Inteligencia Artificial. *Universidad Nacional de Colombia, Trabajo realizado como requisito parcial para btener el grado de*

Magister en Ingeniería - Automatización Industrial. Manizales, Colombia. Obtenido de http://www.bdigital.unal.edu.co/9044/1/7107005.2012.pdf

Lezcano, A. (19 de Marzo de 2014). *SlideShare.* Obtenido de http://es.slideshare.net/aerdna07/perceptrn-simple-redes-neuronales-con-aprendizaje-supervisado

Lieberman, D. A. (Abril de 2012). Aprendizaje y Memoria. Cambridge, Reino Unido, Inglaterra. Obtenido de http://www.investigacionyciencia.es/revistas/investigacion-y-ciencia/numero/439/aprendizaje-y-memoria-10995

Marquéz, J., Pardo, K., & Pizarro, S. (14 de febrero de 2001). Ehternet. *Origen, funcionamiento y rendimiento*. Barranquilla, Colombia.

Martinez, J. (Septiembre de 2011). SISTEMA INTELIGENTE DE DETECCIÓN DE INTRUSIONES. *Trabajo final para obtener el titulo de Magister en Investigación en Informática*. Madrid, España. Obtenido de http://eprints.sim.ucm.es/13504/1/MA_2011-15.pdf

Mayan, D., & Alba, E. (4 de abril de 2005, 2010). *Universidad de Malaga*. Obtenido de Universidad de Matanza: http://www.lcc.uma.es/~eat/courses/cdd-contents/tema5.pdf;http://unalm-construcion2010.wikispaces.com/file/view/l_+X25.pdf

Mehra, R. (Enero de 2013). *Cisco*. Obtenido de IDC Analyze the future [Consulta 8 de nero del 2015]: http://www.cisco.com/web/offer/email/lwj/B3.pdf?keyCode=000652155

Mok, S. C. (2002). Una metodología para el análisis de tráfico de una red de transmisión de datos. *Intersedes*, 144 -153. Obtenido de http://www.intersedes.ucr.ac.cr/ojs/index.php/intersedes/article/viewFile/37/36

monografías.com. (12 de septiembre de 2014). Estándar Abierto. Obtenido de https://es.wikipedia.org/wiki/Est%C3%A1ndar_abierto

MORENO, J. J. (2002). Redes Neuronales Artificiales aplicadas al Análisis de Datos. *UNIVERSITAT DE LES ILLES BALEARS, Trabajo realizado como requisito parcial para obtener el grado de Doctor.* Mallorca, España. Obtenido de http://www.tdx.cat/bitstream/handle/10803/9441/tjjmm1de1.pdf;jsessionid=9B856E444129665FBF163402DE3B2558.tdx1?sequence=1

Murthy, H. A. (30 de junio de 2015). *DocSlide.* Obtenido de http://docslide.us/business/token-bus.html

Naranjo, F. J. (28 de septiembre de 2013). Coceptos básicos de redes TCP/IP. *Universidad Pública de Navarra*. Pamplona, España. Obtenido de https://www.tlm.unavarra.es/~daniel/docencia/lir/lir05_06/slides/1-Conceptosbasicos.pdf

Naranjo, F. J. (28 de septiembre de 2013). *unavarra.es.* Obtenido de Universidad Pública de Navarra: https://www.tlm.unavarra.es/~daniel/docencia/lir/lir05_06/slides/1-Conceptosbasicos.pdf

Navarro, J., Ubilla, G., & Tejeda, M. (28 de julio de 2014). *Universidad Técnica Santa María.* Obtenido de Departamento de Electrónica:

http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G5/Informe%20TLS.pdf

net, a. (2002, p.14). *Token Ring.* Obtenido de Arcesio.net: http://webcache.googleusercontent.com/search?q=cache:WPs2JQVLSnAJ:www.arcesio.net/tokenring/tokenring1a.ppt+&cd=2&hl=es&ct=clnk&gl=ec

novell.com. (Octubre de 2001). *Novell, Inc.* Obtenido de http://www.novell.com/documentation/nw6p/pdfdoc/ipx_enu/ipx_enu.pdf

Oliva, A. A. (Junio de 2013). Universidad Oberta de Catalunya. *Proyecto – Seguridad en redes y sistemas, DETECCIÓN DE INTRUSIONES CON SNORT*. Cataluña, Cataluña, España. Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/22909/5/lalvarezoTFM0613memoria.pdf

P. Barlet, J. S. (Enero de 2004). *SMARTxAC: Sistema de monitorización y análisis de tráfico para la Anella Científica.* Obtenido de RedIRIS.es: http://www.rediris.es/difusion/publicaciones/boletin/66-67/ponencia6.pdf

Perez, S. (noviembre de 2001). *UNT, Facultad Regional de la plata.* Obtenido de Análisis del protocolo IPSec: http://www.frlp.utn.edu.ar/materias/internetworking/apuntes/IPSec/ipsec.pdf

POSSO, G. R. (marzo de 2009, p. 7). DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA E IMPLEMENTACIÓN DE TRES DOMINIOS EN BASE A LA NORMA 27002 PARA EL ÁREA DE HARDWARE EN LA EMPRESA UNIPLEX SYSTEMS S.A. EN QUITO. *Proyecto elaborado como requisito previo para la obtención del título de Ingeniero en Electrónica y Telecomunicaciones*. Quito, Ecuador. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/1371/1/CD-2075.pdf

Raúl, S. P. (Junio de 2002). Análisis de seguridad de la familia de los protocolos TCP/IP y sus servicios asociados. *TCP/IP Security*. México, México: Free Software Foundation, Inc.

Riffo Gutierrez, A. M. (2009). Vulnerabilidad de Redes y Mecanizmos de seguridad. *Universidad Austral de ChileTrabajo de grado presentado como requisito para obtener el Título de Ingeniero Electrónico,*. Valdivia, Valdivia, Chile: Facultad de Ingeniería Civil Electrónica. Obtenido de http://cybertesis.uach.cl/tesis/uach/2009/bmfcir564v/doc/bmfcir564v.pdf

Robbins, C. (2 de Agosto de 2013). *cisco.com*. Obtenido de http://www.cisco.com/cisco/web/support/LA/107/1073/1073935_configuring_decnet_ps6922_TSD_Products_Configuration_Guide_Chapter.pdf

Rojas, A. (30 de abril de 2014). *CCNA Routers & Switches*. Obtenido de suite TCP/IP: http://ciscoswitchrouters.blogspot.com/2014/04/suite-tcpip.html

Romero, M. (05 de Enero de 2006). Lineas de Retardo. España. Obtenido de http://www.biopus.com.ar/matias/materias/apuntes/lineas_de_retardo_delay.pdf

Romero, M. (13 de 07 de 2006). Seguridad en redes y protocolos asociados. Sevilla, España. Obtenido de http://www.dte.us.es/personal/mcromero/docs/ip/tema-seguridad-IP.pdf

Romero, M. d. (13 de julio de 2006). Ingeniería de Protocolos. *Estructura de un protocolo*. Sevilla, España. Obtenido de http://www.dte.us.es/personal/mcromero/docs/ip/tema2-IP.pdf

Sacanamboy, C. (15 de marzo de 2013). *Slide Share.* Obtenido de http://es.slideshare.net/csacanam/fddi-17234254

Santillan, J. (2011). Evolución de los sistemas de detección, prevención y analisis de incidentes. .*SEGURIDAD*, numero-10. Obtenido de http://revista.seguridad.unam.mx/numero-10/evoluci%C3%B3n-de-los-sistemas-de-detecci%C3%B3n-prevenci%C3%B3n-y-an%C3%A1lisis-de-incidentes

Surnoza, R., & Figueira, C. (13 de febrero de 2013). *Universidad Simón Bolivar.* Obtenido de http://ldc.usb.ve/~figueira/cursos/Seguridad/Material/IPsec.pdf

Target, T. (2000 -2015). *Tech Target "Buscar Seguridad"*. Obtenido de http://searchsecurity.techtarget.com/essentialguide/How-to-hone-an-effective-vulnerability-management-program

Torres A. Gabriela C., L. S. (2010). Estudio e implementación de una Metodología de Prevención de intrusos Para Redes LAN. *Sistema de prevención de Intrusos en la Red Coorporativa del Municipio de Riobamba, Escuela Superior Politécnica del Chimborazo, Trabajo realizado como rewuisito parcial para obtener el grado de Ingeniero en Electrónica y Tecnología en Computación*. Riobamba, Chimborazo, Ecuador. Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/383/1/38T00192.pdf

Torres, E. A. (12 de 04 de 2005). Protocolo X.25. *Lenguajes y Ciencias de la Computación*. Malaga, España. Obtenido de http://www.lcc.uma.es/~eat/courses/cdd-contents/tema5.pdf

Tunembaum, A. S. (2003). *REDES DE COMPUTADORAS, 4ta Ed.* Mexico: PEARSON.

Vaca, M. R. (4 de octubre de 2011). *Redes de Datos.* Obtenido de Blog: http://redesdedatos-marquezroserovaca.blogspot.com/2011/10/fddi-cddi.html

Valencia, G. I. (04 de Agosto de 2014). *SEGURIDAD*. Obtenido de Revista No 22. SEGURIDAD, Defensa Digital: http://revista.seguridad.unam.mx/numero22/ciber-seguridad-para-la-educacion-online

Valencia, M., Sanchez, C., & Yáñez, L. (2006). INSTITUTO POLITÉCNICO NACIONAL CENTRO DE INVESTIGACIÓN EN COMPUTACIÓN. *Algoritmo Backpropagation para Redes Neuronales: concepto y aplicaciones(125)*. Obtenido de http://www.repositoriodigital.ipn.mx/bitstream/handle/123456789/8628/Archivo%20que%20incluye%20portada,%20%C3%ADndice%20y%20texto.pdf?sequence=1

Velázquez, J. (13 de Agosto de 2001). *UDLAP*. Obtenido de Colección de Tesis Digitales - Universidad de las Americas Puebla: http://catarina.udlap.mx/u_dl_a/tales/documentos/msp/velazquez_s_j/portada.html

Vila, J., & Chica, J. (Agosto de 2012). *nmap.org*. Obtenido de Guia avanzada de NMAP: http://ns2.elhacker.net/timofonica/manuales/Guia_Avanzada_Nmap.pdf

Villegas, A. G. (19 de enero de 2005 - 2006). Frame Relay - Redes de altas prestaciones. Ciudad Real, España.

Ware, C. (Agosto de 2011). *ASIAP*. Obtenido de IBM: http://www.asiap.org/AsIAP/images/stories/JIAP/jiap2011/Presentaciones/Azul/A1917_IBM.pdf

wildpackets. (2012). *wildpackets.com*. Obtenido de http://www.wildpackets.com/elements/omnipeek/OmniPeek_Network_Analyzer_datasheet.pdf

GLOSARIO DE TÉRMINOS

ABM	Modo balanceado asíncrono
ACLs	Listas de control de accesos
AH	Authentication Header
AIX	Advanced Interactive eXecutive
ANN	Redes Neuronales Artificiales
APs	Puntos de acceso a una red inalámbrica
ARM	Modo de respuesta asíncrono
ARP	Protocolo de Resolución de Direcciones
ARQ	Automatic Repeat-reQuest
ATM	Modo de Transferencia Asíncrona
Backoff	Se produce por una colisión las estaciones las cuales hace callar mediante este algoritmo
BASE	Software de análisis de seguridad basado en Snort.
BECN	Backward Explicit Congestion Notificación
BSD	Berkeley Software Distribution
CCITT	Comité Consultivo Internacional Telegráfico y Telefónico
CDDI	
CERT	Computer Emergency Response Team (Empresa)

Chemotaxis	Algoritmo utilizado en redes recurrentes que se basa en el movimiento de un organismo en respuesta a un estímulo químico, pero la red de Hopfield lo utiliza para identificación de sistemas dinámicos.
CISCO	Es una empresa con sede en San José (Estados Unidos) distribuida a nivel mundial, dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.
CLLM	Consolidated Link Layer Management
COM	Component Objetc Model
CSMA/CD	Acceso Múltiple con Detección de Portadora y Detección de Colisiones
Cuadrante Mágico de Gartner	Análisis de tecnología que realiza la consultora Gartner mediante cuadrantes y los ciclos de sobre expectación, proporcionando consejo relacionado con la industria/sector y el apoyo al gobierno para los profesionales de las TICs.
CVE	Common Vulnerabilities and Exposures
DAC	Digital Audio Card
DAS	Direct Attached Storage
DCE	Equipo de comunicación de datos
DECnet	Digital Equipment Corporation

DES	Data Encryption Standard
DHCP	Protocolo de configuración dinámica de Host
DIX	Digital Equipmen Corporation, Intel and Xerox
DLCI	circuito virtual de conexión de enlace de datos
DLP	Prevención de pérdida de datos para evitar que los usuarios envíen información sensible fuera de la red.
DNS	Domain Name System
DoS o DDoS	Denial of Service ó Distributed Denial of Service
DSA	Direct Selling Association
DTE	Data Terminal Equipment
EIGRP	Es un protocolo de enrutamiento vector distancia que ofrece algoritmos vector distancia y estado de enlace.
ENS	Sistemas de Red Emergentes
ESP	Encapsulating Security Payload
ETD	Equipo Terminal de Datos
Ethical Hacking	Técnicas previstas por una institución para explotar las vulnerabilidades existentes en un sistema objetivo valiéndose de un test de intrusión.
FAL	Foro de Autoridades Locales

FDDI	Interfaz de Datos Distribuida por Fibra, Fiber Distributed Data Interface
FECN	Forward Explicit Congestion Notificación
FHS	Filesystem Hierarchy Standart
Firewall	Es software o hardware que captura información proveniente del internet o una red para comprobar su contenido, este puede bloquear o permitir el paso de esta información dependiendo de la configuración establecida.
Frame Relay	Frame-mode Bearer Service es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual
GPL	General Public License
HAMMING	es un código detector y corrector de errores
HDLC	High-Level Data Link Control, control de enlace de datos de alto nivel
HDLC	High-Level Data Link Control, control de enlace de datos de alto nive
HIPS e NIPS	Host-based Intrusión Prevention Systems e Network Intrusion Prevention System o Sistema de Prevención de Intrusiones a nivel de Red
HMAC	Código de Autenticación de Mensajes basado en Hash

IANA	Internet Assigned Numbers Authority
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detection System ó sistema de detección de intrusiones
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
INPUT	Entradas
IP	Internet Protoco ó Protocolo de internet
IPCOP	es una distribución Linux que implementa un cortafuego
IPS	Intrusion Prevention System ó Sistema de prevención de intrusos
IPX	Internetwork Packet Exchange intercambio de paquetes interred
IPX/SPX	Internetwork Packet Exchange/Sequenced Packet Exchange
ITU-T	Sector de Normalización de las Telecomunicaciones
Keyloggers	Software o dispositivo de hardware que se encarga de registrar las pulsaciones en el teclado para luego memorizarlas en un fichero.
LAN	Local Area Network ó Red de área local
LAP	Link Access Protocol
LAPB	Link Access Procedured Balanced
LMS	error cuadrático medio

Logs	Archivos en los cuales se registran eventos que suceden al utilizar un dispositivo o una aplicación en particular.
LSTM	Bloque de memoria que contiene una o más celdas de memoria utilizadas en la red de Hopfield.
LVQ	Técnica mediante la cual el espacio de entradas es dividida en un número determinado de regiones y cada una de estas está definido por un vector que la caracteriza.
Lyapunov	Es una función que demuestra la estabilidad de un punto fijo en un sistema dinámico o en las ecuaciones diferenciales autónomas.
MAC	media access control ó control de acceso al medio
MD5 o SHA	Message-Digest Algorithm 5 ó Secure Hash Algorithm
MTU	Maximum Transmission Unit
NASL	Nessus Attack Scripting Language, Lenguaje de Scripting de Ataque Nessus
NetBEUI	NETBIOS Extended User Interface
NETBIOS	Network Basic Input/Output System
NMAP	Network Mapper o Mapeador de Redes
NMAP	(Network Mapper o Mapeador de Redes
NMR	Modo de respuesta normal
OSI	Internetwork Operating System

OSPF	Open Shortest Path Firs
PDP-11	Minicomputadoras
PHY	Physical leyer protocol
PKI	infraestructura de clave públic
PMD	Dispersión por Modo de Polarización
PVC	circuitos virtuales permanentes ó
PYME	pequeña y mediana empresa
Pymes	Pequeñas y medianas empresas en las cuales se implementa tecnología y soluciones informáticas.
RDSI	Red digital de servicios integrados
RFCs	Request for Comments
RIP	Protocolo de puerta de enlace interna utilizado por los routers para intercambiar información acerca de las redes que se encuentran conectadas.
ROI	Beneficio que se obtiene por cada unidad monetaria invertida durante un período de tiempo.
RSA	Rivest, Shamir y Adleman
SADB	base de dados de asociación de seguridad
SAS	Social Network Analysis
SI	Seguridad de Información

SLCA	Service Level Agreement
SMARTxAC	Es una plataforma que sirve para el monitoreo y análisis de tráfico para enlaces de alta velocidad.
SMB	Server Message Block
SMT	Scottish Motor Traction
SNA	Systems Network Architecture
software de spamming	Correo o información basura de los mensajes no solicitados, no deseados o remitente no conocido.
SONET	Syncrhonous Optical Network
SPI	Sistemas de Prevención de Intrusos
SPX	Sequenced Packet Exchange
Spyware	Malware que recopila información de un computador para luego transmitirla a una entidad externa sin el consentimiento del propietario.
SSL	Secure Sockets Layer
SSLRP	SSL Record protocol
SVC	circuitos virtuales conmutados
SYN	es un bit de control dentro del segmento TCP, que se utiliza para sincronizar los números de secuencia iniciales ISN
TCO	Costo total de proveer y mantener una solución informática.

TCP	Transmission Control Protocol ó Protocolo de Control de Transmisión
THT	Token Holding Time
TI	Tecnologías de Información
TLS	seguridad de la capa de transporte
Token	Es una serie especial de bits que viajan por las redes token-ring
Token passing	Protocolo utilizado en redes Arcnet y Token Ring el cual está basado en un esquema libre de colisiones
TOS	Type of Servic
TP	Transfer Protocol
TPM	Tipo de red neuronal artificial entrenada utilizando aprendizaje no supervisado que produce una representación discreta del espacio de las muestras de entrada.
TTL	Time To Live
UA	Unnumbered Acknowledged
UDP	User Datagram Protocol ó Protocolo de datagrama de usuario
UTP	Unshielded Twisted Pair
VC	Circuito Virtual
VCC	conexiones se realizan a través de canales virtuales
VLANs	Redes virtuales

VMS	software de gestión de vídeo
VP	Virtual Path
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLANs	wireless local area network
WPA	Wi-Fi Protected Access
XML	Extensible Markup Language

ANEXOS

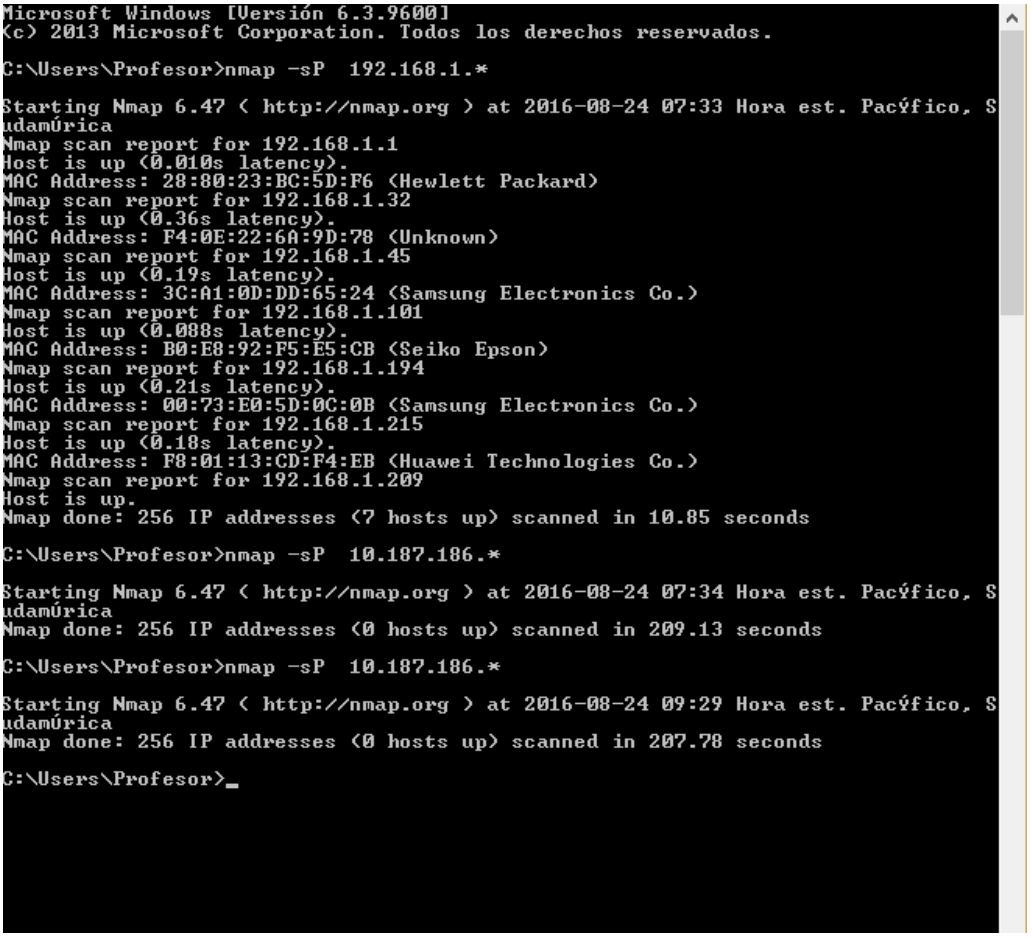
Archivo Snort.config para configurar los preprocesadores

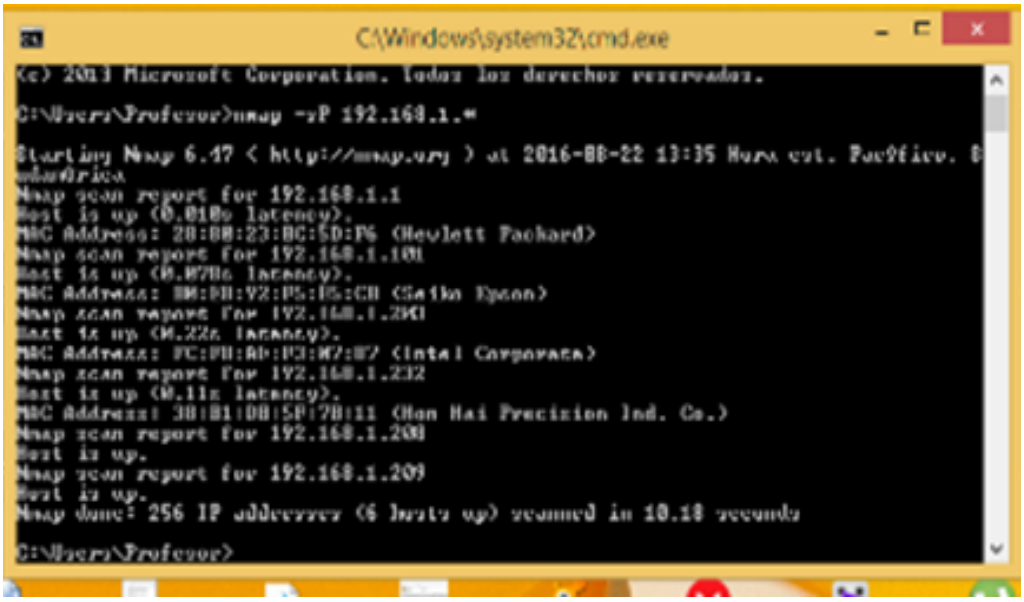
```
#
 config logdir:


##################################################
# Step #3: Configure the base detection engine.  For more
information, see  README.decode
##################################################

# Configure PCRE match limitations
config pcre_match_limit: 3500
config pcre_match_limit_recursion: 1500

# Configure the detection engine  See the Snort Manual,
Configuring Snort - Includes - Config
config detection: search-method ac-split search-optimize max-
pattern-len 20

# Configure the event queue.  For more information, see
README.event_queue
config event_queue: max_queue 8 log 5 order_events content_length

##################################################
## Configure GTP if it is to be used.
## For more information, see README.GTP
##################################################

 config enable_gtp

##################################################
# Per packet and rule latency enforcement
```

Preprocesador SfPortscan

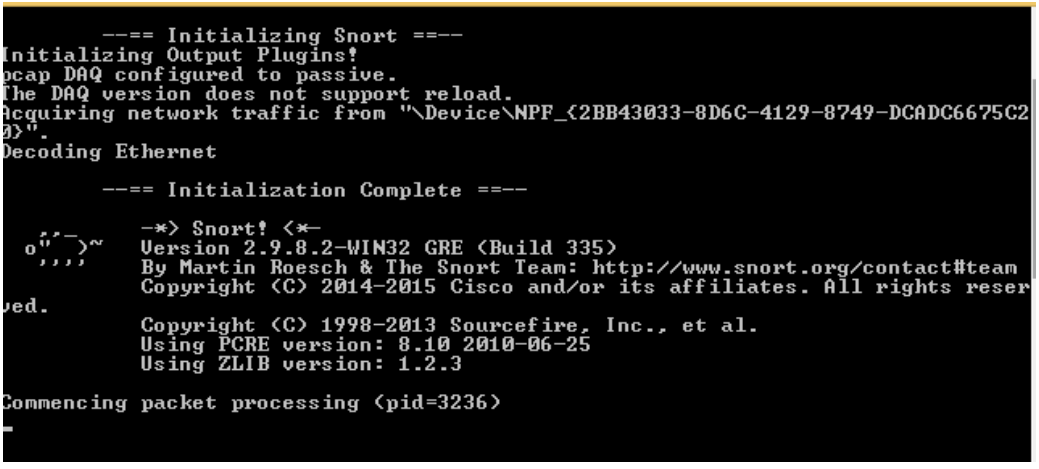
```
    alt_max_command_line_len 246 { SEND SAML SOML AUTH TURN ETRN
DATA RSET QUIT ONEX QUEU STARTTLS TICK TIME TURNME VERB X-EXPS X-
LINK2STATE XADR XAUTH XCIR XEXCH50 XGEN XLICENSE XQUE XSTA XTRN
XUSR } \
    valid_cmds { ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO EMAL
ESAM ESND ESOM ETRN EVFY } \
    valid_cmds { EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT
RCPT RSET SAML SEND SOML } \
    valid_cmds { STARTTLS TICK TIME TURN TURNME VERB VRFY X-ADAT
X-DRCP X-ERCP X-EXCH50 } \
    valid_cmds { X-EXPS X-LINK2STATE XADR XAUTH XCIR XEXCH50 XGEN
XLICENSE XQUE XSTA XTRN XUSR } \
    xlink2state { enabled }

# Portscan detection.  For more information, see
README.sfportscan
 preprocessor sfportscan: proto  { all } memcap { 10000000 }
sense_level { high }

(msg:"Sospechoso Troyano User-Agent (QQ)";

# ARP spoof detection.  For more information, see the Snort
Manual - Configuring Snort - Preprocessors - ARP Spoof
Preprocessor
 preprocessor arpspoof
 preprocessor arpspoof_detect_host: 192.168.0.107
 f0:0f:00:f0:0f:00

# SSH anomaly detection.  For more information, see README.ssh
preprocessor ssh: server_ports { 22 } \
```

Escaneo de direcciones IPS y puertos mediante la herramienta nmap.





Pantalla de Snort iniciando y escaneando amenazadas



```
Len: 50
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
09/29-02:54:43.066207 192.168.132.1:137 -> 192.168.132.255:137
UDP TTL:64 TOS:0x0 ID:102 IpLen:20 DgmLen:78
Len: 50
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
09/29-02:54:43.822626 192.168.132.1:137 -> 192.168.132.255:137
UDP TTL:64 TOS:0x0 ID:103 IpLen:20 DgmLen:78
Len: 50
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
09/29-02:54:44.576060 192.168.132.1:137 -> 192.168.132.255:137
UDP TTL:64 TOS:0x0 ID:104 IpLen:20 DgmLen:78
Len: 50
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
09/29-02:55:07.169628 fe80:0000:0000:0000:dc9f:2fb5:6c8b:ee1d:546 -> ff02:0000:0
000:0000:0000:0000:0001:0002:547
UDP TTL:1 TOS:0x0 ID:0 IpLen:40 DgmLen:141
Len: 93
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
09/29-02:55:08.169626 fe80:0000:0000:0000:dc9f:2fb5:6c8b:ee1d:546 -> ff02:0000:0
000:0000:0000:0000:0001:0002:547
UDP TTL:1 TOS:0x0 ID:0 IpLen:40 DgmLen:141
Len: 93
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
09/29-02:55:10.169713 fe80:0000:0000:0000:dc9f:2fb5:6c8b:ee1d:546 -> ff02:0000:0
000:0000:0000:0000:0001:0002:547
UDP TTL:1 TOS:0x0 ID:0 IpLen:40 DgmLen:141
Len: 93
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
09/29-02:55:14.170269 fe80:0000:0000:0000:dc9f:2fb5:6c8b:ee1d:546 -> ff02:0000:0
000:0000:0000:0000:0001:0002:547
```